INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

March 2026

The total zero-day vulnerabilities count for March month: 793

Command Injection	SQL Injection	Server-Side Request Forgery	Cross-Site Scripting	Prompt Injection	Path Traversal
56	297	42	374	1	23

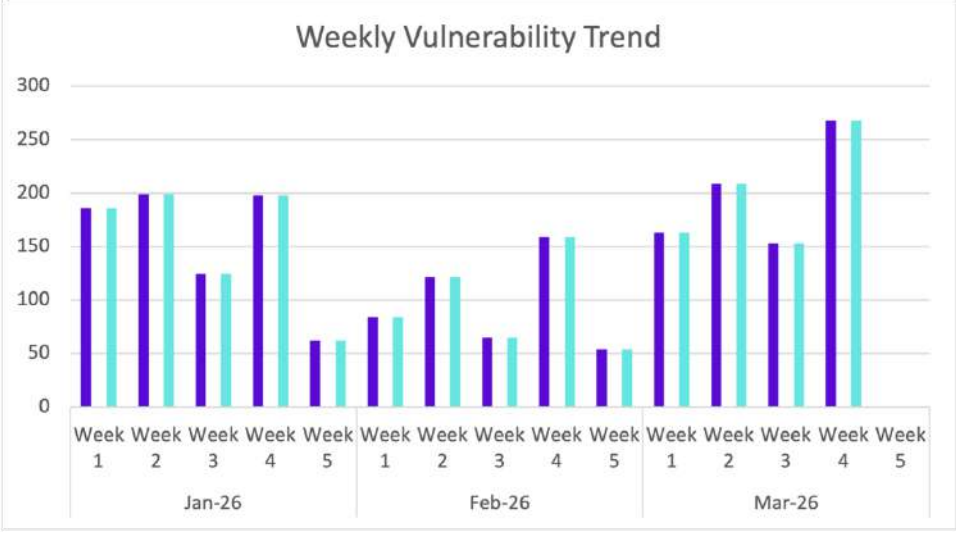
Zero-day vulnerabilities protected through core rules	793
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	793

- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

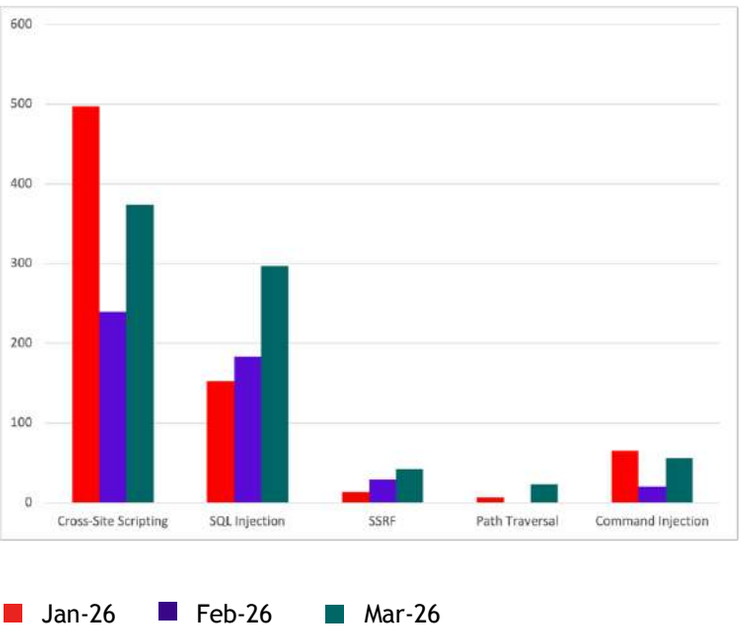
Weekly Vulnerability Trend



of the zero-day vulnerabilities were protected by the core rules in the last month

of the zero-day vulnerabilities were reported by Indusface Scanner in the last month

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-32948	sbt Build Tool — Command Injection via URI Fragment (Windows)	On Windows, sbt passes user-controlled URI fragments (branch, tag, revision) to VCS commands via cmd /c without validation. Shell metacharacters in the fragment allow arbitrary command execution. Fixed in version 1.12.7.	Patched by core rule	Y
CVE-2026-33310	Intake Package — Shell Command Injection via YAML Catalog	Prior to version 2.0.9, shell() expressions in catalog YAML parameter defaults are automatically expanded during parsing. Loading a malicious catalog file can trigger arbitrary command execution on the host. Fixed by disabling getshell by default in 2.0.9.	Patched by core rule	Y
CVE-2026-33648	WWBN AVideo — OS Command Injection via Log File Path	In versions up to 26.0, the restreamer endpoint embeds unsanitized user-controlled values into a log file path, which is then passed directly to exec(). An authenticated attacker can inject shell metacharacters to execute arbitrary commands on the server.	Patched by core rule	Y
CVE-2026-33482	WWBN AVideo — OS Command Injection via FFmpeg Sanitization Bypass	In versions up to 26.0, the sanitizeFFmpegCommand() function strips common shell metacharacters but misses $() (bash command substitution). Since commands run inside a sh	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		-c context, an attacker with a valid encrypted payload can achieve arbitrary command execution on the encoder server.		
CVE-2026-33478	WWBN AVideo — Unauthenticated RCE via CloneSite Plugin Chain	In versions up to 26.0, the CloneSite plugin exposes clone secret keys without authentication, enabling a full database dump. Admin password hashes (MD5) in the dump are trivially crackable. With admin access, an attacker exploits OS command injection in the rsync command to execute arbitrary system commands.	Patched by core rule	Y
CVE-2026-33319	WWBN AVideo — OS Command Injection via LinkedIn Upload URL	Prior to version 26.0, the uploadVideoToLinkedIn() method directly interpolates LinkedIn API response URLs into a shell command without using escapeshellarg(). An attacker who can influence the API response (via MITM or compromised token) can inject arbitrary OS commands executed as the web server user.	Patched by core rule	Y
CVE-2026-32950	SQLBot — SQL Injection Leading to RCE via PostgreSQL COPY	Prior to version 1.7.0, Excel sheet names are concatenated directly into PostgreSQL table names and embedded into COPY SQL statements via f-strings without parameterization. An authenticated attacker can use a two-stage upload technique to inject a TO PROGRAM clause, achieving arbitrary command execution as the postgres user.	Patched by core rule	Y
CVE-2026-32238	OpenEMR — Command Injection in Backup Functionality	Prior to version 8.0.0.2, insufficient input validation in the backup functionality allows authenticated attackers to inject OS commands. Fixed in version 8.0.0.2.	Patched by core rule	Y
CVE-2026-32608	Glances — Command Injection via Mustache Template Variables	Prior to version 4.5.2, Mustache template variables in action commands are populated with runtime monitoring data (process names, container names). When these values contain shell metacharacters, the secure_popen() function splits the command in unintended ways, allowing an attacker who controls a process or container name to inject arbitrary commands.	Patched by core rule	Y
CVE-2026-22179	OpenClaw macOS — Allowlist Bypass via Command Substitution	Prior to version 2026.2.22, the node-host system.run component improperly parses command substitution tokens. Remote attackers can craft shell payloads using command substitution syntax within double-quoted text to bypass the command allowlist and execute arbitrary commands.	Patched by core rule	Y
CVE-2026-28673	xiaoheiFS — RCE via Untrusted Plugin Binary	In versions up to 0.3.15, the plugin system allows admins to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Execution	upload a ZIP containing a binary and manifest.json. The server executes the binary specified in the manifest without validating its contents, leading to Remote Code Execution. Fixed in version 0.4.0.		
CVE-2026-27811	Roxy-WI — Command Injection in Config Compare Endpoint	Prior to version 8.2.6.3, user input to the /config/compare endpoint is directly formatted into a template string that is subsequently executed as a system command. Authenticated attackers can inject arbitrary OS commands on the application host.	Patched by core rule	Y
CVE-2026-4253	Tenda AC8 — OS Command Injection via wans.policy.list1	In Tenda AC8 firmware 16.03.50.11, the route_set_user_policy_rule function in /cgi-bin/UploadCfg does not validate the wans.policy.list1 argument, allowing remote attackers to inject and execute arbitrary OS commands via the web interface.	Patched by core rule	Y
CVE-2026-4209	D-Link DNS Series — Command Injection in account_mgr.cgi	Multiple D-Link DNS NAS devices up to firmware 20260205 are vulnerable to command injection in the account management CGI functions (cgi_create_import_users, cgi_user_add, cgi_group_add, and others). The attack can be initiated remotely and a public exploit is available.	Patched by core rule	Y
CVE-2026-4207	D-Link DNS Series — Command Injection in system_mgr.cgi	Multiple D-Link DNS NAS devices up to firmware 20260205 are vulnerable to command injection in the system management CGI functions (cgi_device, cgi_sms_test, cgi_firmware_upload, cgi_ntp_time). The attack can be initiated remotely and a public exploit is available.	Patched by core rule	Y
CVE-2026-4206	D-Link DNS Series — Command Injection in dsk_mgr.cgi	Multiple D-Link DNS NAS devices up to firmware 20260205 are vulnerable to command injection in disk management CGI functions (FMT_rebuild_diskmgr, FMT_create_diskmgr, ScanDisk_run_e2fsck). The attack can be initiated remotely and a public exploit is available.	Patched by core rule	Y
CVE-2026-4205	D-Link DNS Series — Command Injection in app_mgr.cgi	Multiple D-Link DNS NAS devices up to firmware 20260205 are vulnerable to command injection in app management CGI functions (cgi_refresh_db, FTP_Server_BlockIP_Add, FTP_Server_BlockIP_Del). The attack can be initiated remotely and a public exploit is available.	Patched by core rule	Y
CVE-2026-4203	D-Link DNS Series — Command Injection in network_mgr.cgi	Multiple D-Link DNS NAS devices up to firmware 20260205 are vulnerable to command injection in network management CGI functions (cgi_portforwarding_add, cgi_dhcpd, cgi_ddns, cgi_ip, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		others). The attack can be initiated remotely and a public exploit is available.		
CVE-2026-4197	D-Link DNS Series — Command Injection in download_mgr.cgi	Multiple D-Link DNS NAS devices up to firmware 20260205 are vulnerable to command injection in download manager CGI functions (RSS_Get_Update_Status, RSS_Add, RSS_Update, and others). The attack can be initiated remotely and a public exploit is available.	Patched by core rule	Y
CVE-2026-4196	D-Link DNS Series — Command Injection in remote_backup.cgi	Multiple D-Link DNS NAS devices up to firmware 20260205 are vulnerable to command injection in remote backup CGI functions (cgi_recovery, cgi_backup_now, cgi_set_schedule, cgi_set_rsync_server). The attack can be initiated remotely and a public exploit is available.	Patched by core rule	Y
CVE-2026-4195	D-Link DNS Series — Command Injection in wizard_mgr.cgi	Multiple D-Link DNS NAS devices up to firmware 20260205 are vulnerable to command injection in the wizard manager CGI (/cgi-bin/wizard_mgr.cgi). The attack can be initiated remotely and a public exploit is available.	Patched by core rule	Y
CVE-2026-32260	Deno — Command Injection via node:child_process Shell Mode Bypass	In versions 2.7.0 to 2.7.1, the node:child_process polyfill has a priority bug: arguments containing $VAR patterns are wrapped in double quotes instead of single quotes. Double quotes do not suppress backtick command substitution in POSIX sh, allowing attackers who control spawn arguments with shell:true to execute arbitrary OS commands, bypassing Deno's permission system. Fixed in 2.7.2.	Patched by core rule	Y
CVE-2026-26793	GL-iNet GL-AR300M16 — Command Injection via set_config Function	GL-iNet GL-AR300M16 v4.3.11 contains a command injection vulnerability in the set_config function. Attackers can execute arbitrary commands by sending a crafted input to the affected function.	Patched by core rule	Y
CVE-2026-26795	GL-iNet GL-AR300M16 — Command Injection via get_system_log Module	GL-iNet GL-AR300M16 v4.3.11 contains a command injection vulnerability in the module parameter of the M.get_system_log function. Attackers can execute arbitrary commands via a crafted input.	Patched by core rule	Y
CVE-2026-26792	GL-iNet GL-AR300M16 — Multiple Command Injections in set_upgrade	GL-iNet GL-AR300M16 v4.3.11 contains multiple command injection vulnerabilities in the set_upgrade function across several parameters (modem_url, target_version, current_version, firmware_upload, hash_type, hash_value, upgrade_type). Attackers can execute arbitrary commands via crafted input to any of these parameters.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-26791	GL-iNet GL-AR300M16 — Command Injection via enable_echo_server Port	GL-iNet GL-AR300M16 v4.3.11 contains a command injection vulnerability in the port parameter of the enable_echo_server function. Attackers can execute arbitrary commands via a crafted input.	Patched by core rule	Y
CVE-2026-3964	OpenAkita — OS Command Injection via Chat API Message Argument	In OpenAkita up to version 1.24.3, the run function in the Chat API Endpoint does not validate the Message argument, leading to OS command injection. The attack is restricted to local execution but the exploit is publicly available.	Patched by core rule	Y
CVE-2026-31975	Cloud CLI (Claude Code UI) — OS Command Injection via WebSocket Shell	Prior to version 1.25.0, the server/index.js component takes projectPath and initialCommand directly from WebSocket message payloads and interpolates them into a bash command string without sanitization. A secondary injection vector exists via unsanitized sessionId. Allows arbitrary OS command execution. Fixed in 1.25.0.	Patched by core rule	Y
CVE-2026-32063	OpenClaw — Command Injection via Systemd Unit File Newline Injection	Version 2026.2.19-2 prior to 2026.2.21 does not validate CR/LF characters in environment variable values used in systemd unit file generation. An attacker who can influence config.env.vars and trigger a service install or restart can inject arbitrary systemd directives and execute commands with the privileges of the OpenClaw gateway service user.	Patched by core rule	Y
CVE-2026-28292	simple-git — RCE via Prior CVE Fix Bypass	Versions 3.15.0 through 3.32.2 contain a bypass for the fixes introduced for CVE-2022-25860 and CVE-2022-25912, enabling full remote code execution on the host. Fixed in version 3.23.0.	Patched by core rule	Y
CVE-2026-25041	Budibase — PostgreSQL Integration Command Injection	In version 3.23.22 and earlier, the PostgreSQL integration constructs shell commands using unsanitized user-controlled configuration values including database name, host, and password. These parameters are directly interpolated into shell commands in packages/server/src/integrations/postgres.ts.	Patched by core rule	Y
CVE-2026-3696	Totolink N300RH — OS Command Injection in setWiFiWpsConfig	Totolink N300RH firmware 6.1c.1353_B20190305 contains an OS command injection vulnerability in the setWiFiWpsConfig function of /cgi-bin/cstecgi.cgi. The attack can be initiated remotely and a public exploit is available.	Patched by core rule	Y
CVE-2026-30861	WeKnora — Unauthenticated RCE via MCP stdio Configuration	From version 0.2.5 to before 0.2.10, the MCP stdio configuration validation can be bypassed using the -p flag with npx node, circumventing the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		command whitelist. Since the application allows unrestricted user registration, any attacker can create an account and exploit this flaw to execute arbitrary commands with the application's privileges. Fixed in 0.2.10.		
CVE-2026-28507	Idno — RCE via Chained File Write and Template Path Traversal	Prior to version 1.6.4, a remote code execution vulnerability exists through a chain of file write and template path traversal. Fixed in version 1.6.4.	Patched by core rule	Y
CVE-2026-26478	Mobvoi Tichome Mini — RCE via Crafted UDP Datagram	Mobvoi Tichome Mini smart speakers (models 012-18853 and 027-58389) contain a shell command injection vulnerability that allows remote attackers to send a specially crafted UDP datagram and execute arbitrary shell code as the root account.	Patched by core rule	Y
CVE-2026-28774	IDC SFX SuperFlex — OS Command Injection via Traceroute Flags	The web-based Traceroute diagnostic utility in IDC SFX Series SuperFlex Satellite Receiver Web Management Interface version 101 does not sanitize the flags parameter. An authenticated attacker can inject shell metacharacters such as the pipe operator to execute arbitrary OS commands with root privileges.	Patched by core rule	Y
CVE-2026-28773	IDC SFX SuperFlex — OS Command Injection via Ping IPaddr Parameter	The web-based Ping diagnostic utility in IDC SFX Series SuperFlex Satellite Receiver Web Management Interface version 101 insecurely parses the IPaddr parameter. Server-side semicolon exclusion checks can be bypassed using alternate shell metacharacters such as the pipe operator. An authenticated attacker can execute arbitrary shell commands with root privileges.	Patched by core rule	Y
CVE-2026-26279	Froxlor — Root RCE via Disabled Email Validation in Cron Job	Prior to version 2.3.4, a typo (== instead of =) in Froxlor's input validation completely disables email format checking for settings fields declared as email type. An authenticated admin can store arbitrary strings in panel.adminmail, which is later concatenated into a shell command executed as root by a cron job. The pipe character is explicitly whitelisted, enabling full root-level RCE. Fixed in 2.3.4.	Patched by core rule	Y
CVE-2026-3485	D-Link DIR-868L — OS Command Injection via SSDP ST Argument	D-Link DIR-868L firmware 110b03 contains an OS command injection vulnerability in the SSDP Service's sub_1BF84 function. Manipulation of the ST argument allows remote attackers to execute arbitrary commands. This product is no longer supported by the manufacturer.	Patched by core rule	Y
CVE-2025-67840	Cohesity TranZman — Multiple Authenticated OS Command Injections	TranZman 4.0 Build 14614 through TZM_1757588060_SEP2025_FU	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		LL.depot directly concatenates user-controlled parameters into system commands across multiple API endpoints (Scheduler, Actions). An authenticated admin can inject shell metacharacters via a proxy to achieve RCE with root privileges, bypassing the CLISH restricted shell. Unpatched as of the latest available build.		
CVE-2025-63911	Cohesity TranZman — Authenticated Command Injection	TranZman Migration Appliance Release 4.0 Build 14614 contains an authenticated command injection vulnerability allowing arbitrary command execution on the appliance.	Patched by core rule	Y
CVE-2026-2256	ModelScope ms-agent — OS Command Injection via Prompt-Derived Input	In ms-agent versions v1.6.0rc1 and earlier, prompt-derived input is passed to OS command execution without sanitization. An attacker can craft prompts to execute arbitrary operating system commands.	Patched by core rule	Y
CVE-2026-24105	Tenda AC15 — Command Injection via usbPartitionName in doSystemCmd	In Tenda AC15V1.0 firmware V15.03.05.18_multi, the value of usbPartitionName in goform/formsetUsbUnload is not validated before being passed to doSystemCmd, potentially allowing arbitrary command injection.	Patched by core rule	Y
CVE-2026-24101	Tenda AC15 — Command Injection via formSetIptv s1_1 Parameter	In Tenda AC15V1.0 firmware V15.03.05.18_multi, when specific conditions are met, the s1_1 parameter in goform/formSetIptv is passed into sub_B0488 and concatenated into doSystemCmd without validation, allowing arbitrary command injection.	Patched by core rule	Y
CVE-2025-50197	Chamilo LMS — OS Command Injection via new_language Parameter	Prior to version 1.11.30, the new_language POST parameter in /main/admin/sub_language_ajax.inc.php is not sanitized, enabling OS command injection by authenticated attackers. Fixed in version 1.11.30.	Patched by core rule	Y
CVE-2025-50196	Chamilo LMS — OS Command Injection via main_database Parameter	Prior to version 1.11.30, the main_database POST parameter in /plugin/vchamilo/views/editinstance.php is not sanitized, enabling OS command injection by authenticated attackers. Fixed in version 1.11.30.	Patched by core rule	Y
CVE-2025-50195	Chamilo LMS — OS Command Injection in manage.controller.php	Prior to version 1.11.30, an OS command injection vulnerability exists in /plugin/vchamilo/views/manage.controller.php. Fixed in version 1.11.30.	Patched by core rule	Y
CVE-2025-50194	Chamilo LMS — OS Command Injection in check_parse_lang.php	Prior to version 1.11.30, an OS command injection vulnerability exists in /main/cron/lang/check_parse_lang.php. Fixed in version 1.11.30.	Patched by core rule	Y
CVE-2025-50193	Chamilo LMS — OS Command	Prior to version 1.11.30, the	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Injection via to_main_database Parameter	to_main_database POST parameter in /plugin/vchamilo/views/import.php is not sanitized, enabling OS command injection by authenticated attackers. Fixed in version 1.11.30.	rule	
CVE-2026-24107	Tenda W20E — Command Injection via usbPartitionName in doSystemCmd	In Tenda W20E firmware V4.0br_V15.11.0.6, the usbPartitionName value is not validated before being passed directly to doSystemCmd, allowing critical command injection vulnerabilities.	Patched by core rule	Y
CVE-2026-28517	openDCIM — OS Command Injection via dot Config in report_network_map	openDCIM version 23.04 through commit 4467e9c4 retrieves the dot configuration parameter from the database and passes it directly to exec() in report_network_map.php without validation. If an attacker can modify the fac_Config.dot value, they can execute arbitrary commands in the web server process context.	Patched by core rule	Y
CVE-2026-28409	WeGIA — RCE via Crafted Backup Filename in Database Restore	Prior to version 3.6.5, an attacker with administrative access can execute arbitrary OS commands by uploading a backup file with a specially crafted filename through the database restore functionality. Fixed in version 3.6.5.	Patched by core rule	Y
CVE-2026-3301	Totolink N300RH — OS Command Injection via webWlanIdx Parameter	Totolink N300RH firmware 6.1c.1353_B20190305 contains an OS command injection vulnerability in the setWebWlanIdx function of /cgi-bin/cstecgi.cgi. Manipulation of the webWlanIdx argument allows remote attackers to execute arbitrary commands.	Patched by core rule	Y
CVE-2026-28207	Zen C Compiler — Command Injection via Crafted Output Filename	Prior to version 0.4.2, the Zen C compiler constructs a shell command by concatenating user-controlled output filenames and passes it to system(). Shell metacharacters in the -o argument are interpreted by the shell, allowing arbitrary command execution with the privileges of the user running the compiler. Fixed in 0.4.2 by replacing system() with internal argument handling.	Patched by core rule	Y
CVE-2026-27635	Manyfold — RCE via Shell Metacharacter in ZIP Upload Filename	Prior to version 0.133.0, when model render generation is enabled, an authenticated user can upload a ZIP file containing a filename with shell metacharacters. The filename reaches a Ruby backtick call unsanitized, enabling Remote Code Execution. Fixed in version 0.133.0.	Patched by core rule	Y
CVE-2026-22719	VMware Aria Operations — Unauthenticated Command Injection RCE	VMware Aria Operations contains a command injection vulnerability exploitable by unauthenticated attackers while support-assisted product migration is in progress.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Successful exploitation can lead to remote code execution. Patches are available in the Broadcom Security Advisory VMSA-2026-0001 Response Matrix.		

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33309	Langflow — Arbitrary File Write via Multipart Upload Filename Bypass	In versions 1.2.0 through 1.8.1, the POST /api/v2/files/ endpoint is vulnerable to arbitrary file write. The multipart upload filename bypasses the HTTP-layer path-parameter guard because the underlying LocalStorageService lacks boundary containment checks. Authenticated attackers can write files anywhere on the host, leading to Remote Code Execution. Fixed in version 1.9.0.	Patched by core rule	Y
CVE-2026-33242	Salvo Rust Framework — Path Traversal via Unencoded ../ in Proxy Component	In versions 0.39.0 through 0.89.2, the salvo-proxy component's encode_url_path function fails to normalize ../ sequences and forwards them verbatim to upstream servers. An unauthenticated attacker can bypass proxy routing constraints and access unintended backend paths including protected endpoints and admin dashboards. Fixed in version 0.89.3.	Patched by core rule	Y
CVE-2026-33293	WWBN AVideo — Arbitrary File Deletion via Path Traversal in CloneSite	Prior to version 26.0, the deleteDump parameter in plugin/CloneSite/cloneServer.json.php is passed directly to unlink() without path sanitization. An attacker with valid clone credentials can use ../ sequences to delete arbitrary files including configuration.php, causing denial of service or enabling further compromise. Fixed in version 26.0.	Patched by core rule	Y
CVE-2026-33292	WWBN AVideo — Unauthenticated Video Access via Path Traversal in HLS Endpoint	Prior to version 26.0, the HLS streaming endpoint (view/hls.php) uses the videoDirectory parameter in two divergent code paths — one for authorization (truncates at first / segment) and one for file access (preserves ../ sequences). This split-oracle condition allows unauthenticated attackers to stream any private or paid video. Fixed in version 26.0.	Patched by core rule	Y
CVE-2019-25610	NetNumber Titan Master — Path Traversal via Base64-Encoded Sequences in drp Endpoint	NetNumber Titan Master 7.9.1 contains a path traversal vulnerability in the drp endpoint. Authenticated users can inject base64-encoded ../ sequences into the path parameter to bypass authorization and download arbitrary files from the server, including sensitive system files such as /etc/shadow.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33476	SiYuan — Unauthenticated Path Traversal via /appearance/* Endpoint	Prior to version 3.6.2, the SiYuan kernel exposes an unauthenticated file-serving endpoint at /appearance/*filepath. Authentication checks explicitly exclude this endpoint and path sanitization is insufficient, allowing unauthenticated attackers to read arbitrary files accessible to the server process. Fixed in version 3.6.2.	Patched by core rule	Y
CVE-2026-27625	Stirling-PDF — Arbitrary File Write via ZIP Entry Path Traversal	Prior to version 2.5.2, the /api/v1/convert/markdown/pdf endpoint extracts user-supplied ZIP entries without validating paths. Any authenticated user can write files outside the intended temporary working directory with the privileges of the stirlingpdfuser process account. Fixed in version 2.5.2.	Patched by core rule	Y
CVE-2026-32938	SiYuan — Sensitive File Exfiltration via file:// Link Copy and Asset API	In versions 3.6.0 and below, the /api/lute/html2BlockDOM endpoint copies local files referenced by file:// links in pasted HTML into the workspace assets directory without validating against a sensitive-path list. Combined with GET /assets/*path (authentication only), a visitor can trigger the desktop kernel to copy and then read any sensitive file accessible to the process. Fixed in version 3.6.1.	Patched by core rule	Y
CVE-2026-32808	pyLoad — Arbitrary File Deletion via Path Traversal in 7z Archive Extraction	Prior to version 0.5.0b3.dev97, pyLoad derives archive entry names from 7z listing output during password verification of encrypted archives with non-encrypted headers, treating them as filesystem paths without constraining to the extraction directory. This allows arbitrary file deletion outside the extraction directory. Fixed in version 0.5.0b3.dev97.	Patched by core rule	Y
CVE-2026-32750	SiYuan — Arbitrary File Read via Unsanitized localPath in importStdMd API	In versions 3.6.0 and below, POST /api/import/importStdMd passes the localPath parameter directly to model.ImportFromLocalPath with no path validation. The function recursively reads all files under the given path and stores their contents as searchable notes accessible to all workspace users, including Publish Service Reader accounts. Fixed in version 3.6.1.	Patched by core rule	Y
CVE-2026-32747	SiYuan — Admin File Exfiltration via globalCopyFiles API with Incomplete Blocklist	In versions 3.6.0 and below, the globalCopyFiles API reads source files using filepath.Abs() with no workspace boundary check. The sensitive-path blocklist in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		util.IsSensitivePath() omits /proc/, /run/secrets/, and home directory dotfiles. An admin can copy /proc/1/environ or Docker secrets into the workspace and read them via the standard file API. In containerized deployments, this exposes all injected secrets and environment variables. Fixed in version 3.6.1.		
CVE-2026-25770	Wazuh — Root RCE via Cluster Protocol File Write and logcollector Config Injection	In versions 3.9.0 through 4.14.2, the wazuh-clusterd service allows authenticated cluster nodes to write arbitrary files to the manager filesystem as the wazuh user. Due to insecure default permissions, the wazuh user can overwrite ossec.conf. The wazuh-logcollector service (running as root) parses this configuration and executes injected commands, enabling full root RCE from cluster credentials. Fixed in version 4.14.3.	Patched by core rule	Y
CVE-2026-32709	PX4 Autopilot — Unauthenticated Path Traversal in MAVLink FTP Implementation	Prior to version 1.17.0-rc2, the MAVLink FTP implementation allows any MAVLink peer to read, write, create, delete, and rename arbitrary files on the flight controller without authentication. On NuttX targets, the FTP root is an empty string, meaning paths are passed to syscalls unsanitized. On POSIX targets, write-path validation unconditionally returns true. A TOCTOU race condition further bypasses the only existing guard on NuttX. Fixed in version 1.17.0-rc2.	Patched by core rule	Y
CVE-2026-30853	calibre — Arbitrary File Write via Path Traversal in RocketBook (.rb) Plugin	Prior to version 9.5.0, the RocketBook (.rb) input plugin does not validate paths during file extraction, allowing an attacker to write arbitrary files to any path writable by the calibre process when a user opens or converts a crafted .rb file. The same bug class was fixed for PDB readers in CVE-2026-26065 but was never applied to the RB reader. Fixed in version 9.5.0.	Patched by core rule	Y
CVE-2026-30958	OneUptime — Unauthenticated Path Traversal in /workflow/docs/:componentName Endpoint	Prior to version 10.0.21, the componentName route parameter in the /workflow/docs/:componentName endpoint is concatenated directly into a file path passed to res.sendFile() without sanitization or authentication middleware. Unauthenticated attackers can read arbitrary files from the server filesystem. Fixed in version	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		10.0.21.		
CVE-2026-30942	Flare — Authenticated Path Traversal in Avatar Filename Parameter	Prior to version 1.7.3, the filename URL parameter in /api/avatars/[filename] is passed to path.join() without sanitization. URL-encoded ../ sequences allow any authenticated user to escape the uploads/avatars/ directory and read any file accessible to the Next.js process under /app/. On instances with open registration enabled (the default), self-registration immediately enables exploitation. Fixed in version 1.7.3.	Patched by core rule	Y
CVE-2026-30869	SiYuan — Path Traversal in /export Endpoint Leaking API Token and Secrets	Prior to version 3.5.10, double-encoded traversal sequences in the /export endpoint allow attackers to read arbitrary files from the server filesystem. Sensitive files such as conf/conf.json contain the API token, cookie signing key, and workspace authentication code. Leaking these secrets may enable administrative API access and in certain deployments can be chained into Remote Code Execution. Fixed in version 3.5.10.	Patched by core rule	Y
CVE-2026-30240	Budibase — Path Traversal in PWA ZIP Endpoint Exposes Environment Secrets	In version 3.31.5 and earlier, the POST /api/pwa/process-zip endpoint reads attacker-specified files via unsanitized path.join() with user-controlled input from icons.json inside an uploaded ZIP. An authenticated user with builder privileges can read arbitrary server files including /proc/1/environ, which contains JWT secrets, database credentials, encryption keys, and API tokens. Contents are uploaded to the object store and retrievable via signed URLs. Fixed in a later release.	Patched by core rule	Y
CVE-2025-70231	D-Link DIR-513 — Path Traversal via FILECODE Parameter in Login Endpoint	D-Link DIR-513 version 1.10 fails to filter the FILECODE parameter value in /goform/getAuthCode, which is reached during POST requests to /goform/formLogin for verification code processing. The lack of filtering results in a path traversal vulnerability.	Patched by core rule	Y
CVE-2026-28769	IDC SFX SuperFlex — Path Traversal via file Parameter in Logging CGI	In the IDC SFX Series SuperFlex Satellite Receiver Web Management Interface version 101, the file parameter in /IDC_Logging/checkifdone.cgi is not validated. Authenticated attackers can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulate this parameter using directory traversal sequences to enumerate and access arbitrary files on the underlying filesystem.		
CVE-2026-28414	Gradio — Absolute Path Traversal on Windows via Python 3.13 os.path.isabs Change	Prior to version 6.7, Gradio apps running on Windows with Python 3.13+ are vulnerable to absolute path traversal. Python 3.13 changed os.path.isabs so root-relative paths like /windows/win.ini are no longer considered absolute, breaking Gradio's safe path-joining logic. Unauthenticated attackers can read arbitrary files from the Gradio server even when authentication is enabled. Fixed in version 6.7.	Patched by core rule	Y
CVE-2026-27734	Beszel — Path Traversal in Container API via Unsanitized Docker URL Construction	Prior to version 0.18.4, the hub passes user-supplied container query parameters to agents without validation. Agents construct Docker Engine API URLs using fmt.Sprintf with raw values instead of url.PathEscape(). Since Go's http.Client does not sanitize ../ sequences from Unix socket URL paths, authenticated users (including readonly role) can traverse to arbitrary Docker API endpoints on agent hosts, exposing sensitive infrastructure details. Fixed in version 0.18.4.	Patched by core rule	Y
CVE-2026-24488	OpenEMR — Arbitrary File Exfiltration via Unsanitized File Path in Fax Endpoint	In versions up to and including 8.0.0, the fax sending endpoint accepts arbitrary file paths from user input and streams file contents to the fax gateway without path restrictions or authorization checks. Any authenticated user can read and transmit any server file including database credentials, patient documents, system files, and source code to an attacker-controlled fax number. No patch available at time of disclosure.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-32539	PublishPress Revisions — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PublishPress PublishPress Revisions revisionary allows Blind SQL Injection.This issue affects PublishPress Revisions: from n/a through <= 3.7.23.	Patched by core rule	Y
CVE-2026-32534	JS Help Desk — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in JoomSky JS Help Desk js-support-ticket allows Blind SQL Injection.This issue affects JS Help Desk: from n/a through <= 3.0.3.	Patched by core rule	Y
CVE-2026-32516	Miraculous Core Plugin — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav Miraculous Core Plugin miraculouscore allows Blind SQL Injection.This issue affects Miraculous Core Plugin: from n/a through < 2.1.2.	Patched by core rule	Y
CVE-2026-32499	ChatBot — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in QuantumCloud ChatBot chatbot allows Blind SQL Injection.This issue affects ChatBot: from n/a through <= 7.7.9.	Patched by core rule	Y
CVE-2026-31920	Product Rearrange for WooCommerce — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Devteam HaywoodTech Product Rearrange for WooCommerce products-rearrange-woocommerce allows Blind SQL Injection.This issue affects Product Rearrange for WooCommerce: from n/a through <= 1.2.2.	Patched by core rule	Y
CVE-2026-27039	WZone — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team WZone woozone allows Blind SQL Injection.This issue affects WZone: from n/a through <= 14.0.31.	Patched by core rule	Y
CVE-2026-25377	Addon Jobsearch Chat — SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in eyecix Addon Jobsearch Chat addon-jobsearch-chat allows SQL Injection.This issue affects Addon Jobsearch Chat: from n/a through <= 3.0.	Patched by core rule	Y
CVE-2026-25371	Lumise Product Designer — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in King-Theme Lumise Product Designer lumise	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows Blind SQL Injection.This issue affects Lumise Product Designer: from n/a through < 2.0.9.		
CVE-2026-25340	Jobmonster — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NooTheme Jobmonster noo-jobmonster allows Blind SQL Injection.This issue affects Jobmonster: from n/a through < 4.8.4.	Patched by core rule	Y
CVE-2026-25007	ElementInvader Addons for Elementor — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Element Invader ElementInvader Addons for Elementor elementinvader-addons-for-elementor allows Blind SQL Injection.This issue affects ElementInvader Addons for Elementor: from n/a through <= 1.4.2.	Patched by core rule	Y
CVE-2026-24993	Advanced WooCommerce Product Sales Reporting — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPFactory Advanced WooCommerce Product Sales Reporting webd-woocommerce-advanced-reporting-statistics allows Blind SQL Injection.This issue affects Advanced WooCommerce Product Sales Reporting: from n/a through <= 4.1.3.	Patched by core rule	Y
CVE-2026-24977	Organici Library — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NooTheme Organici Library noo-organici-library allows Blind SQL Injection.This issue affects Organici Library: from n/a through <= 2.1.2.	Patched by core rule	Y
CVE-2026-22484	Lisfinity Core — SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in pebas Lisfinity Core lisfinity-core allows SQL Injection.This issue affects Lisfinity Core: from n/a through <= 1.5.0.	Patched by core rule	Y
CVE-2024-58341	OpenCart Core 4.0.2.3 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate data...	Attackers can send GET requests to the product search endpoint with malicious 'search' values to extract sensitive database information using boolean-based blind or time-based blind SQL injection techniques.	Patched by core rule	Y
CVE-2026-4781	SourceCodester Sales and Inventory System — SQL Injection	Executing a manipulation of the argument sid can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-4780	SourceCodester Sales and Inventory System — SQL Injection via sid	Impacted is an unknown function of the file update_out_standing.php of the component HTTP GET Parameter Handler. Performing a manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sid results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.		
CVE-2026-4779	SourceCodester Sales and Inventory System — SQL Injection	Such manipulation of the argument sid leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-4778	SourceCodester Sales and Inventory System — SQL Injection via sid	This manipulation of the argument sid causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-4777	SourceCodester Sales and Inventory System — SQL Injection via searchtxt	The manipulation of the argument searchtxt results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2019-25643	eNdonesia Portal v8.7 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute...	Attackers can send GET requests to banners.php with crafted SQL payloads in the bid parameter to extract sensitive database information from the INFORMATION_SCHEMA tables.	Patched by core rule	Y
CVE-2019-25642	Bootstrapy CMS contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitr...	Attackers can inject SQL payloads into the thread_id parameter of forum-thread.php, the subject parameter of contact-submit.php, the post-id parameter of post-new-submit.php, and the thread-id parameter to extract sensitive database information or cause denial of service.	Patched by core rule	Y
CVE-2019-25641	Netartmedia Vlog System contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate d...	Attackers can send POST requests to index.php with malicious email values in the forgotten_password module to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25640	Inout Article Base CMS contains SQL injection vulnerabilities that allow unauthenticated attackers to manipulate data...	Attackers can inject SQL code using XOR-based payloads in GET requests to portalLogin.php to extract sensitive database information or cause denial of service through time-based attacks.	Patched by core rule	Y
CVE-2019-25639	Matrimony Website Script M-Plus contains multiple SQL injection vulnerabilities that allow unauthenticated attackers ...	Attackers can inject malicious SQL payloads into parameters like txtGender, religion, Fage, and cboCountry across simplesearch_results.php, advsearch_results.php, specialcase_results.php, locational_results.php, and registration2.php to extract sensitive database information or execute arbitrary SQL commands.	Patched by core rule	Y
CVE-2019-25638	Meeplace Business Review Script contains an SQL injection vulnerability that allows unauthenticated attackers to exec...	Attackers can send GET requests to the addclick.php endpoint with crafted SQL payloads in the 'id' parameter to extract sensitive database information or cause denial of service.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2019-25636	Zeeways Jobsite CMS contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate datab...	Attackers can send crafted requests to news_details.php, jobs_details.php, or job_cmp_details.php with malicious 'id' values using GROUP BY and CASE statements to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25635	Zeeways Matrimony CMS contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to manipul...	Attackers can inject SQL code via the up_cast, s_mother, and s_religion parameters to extract sensitive database information using time-based or error-based techniques.	Patched by core rule	Y
CVE-2026-4662	The JetEngine plugin for WordPress is vulnerable to SQL Injection via the `listing_load_more` AJAX action in all vers...	Vulnerability via the `listing_load_more` AJAX action due to insufficient input sanitization or output escaping. Affects versions up to and including 3.8.6.1..	Patched by core rule	Y
CVE-2026-3079	The LearnDash LMS plugin for WordPress is vulnerable to blind time-based SQL Injection via the 'filters[orderby_order...	Vulnerability via the 'filters[orderby_order]' parameter in the 'learndash_propanel_template' AJAX action due to insufficient input sanitization or output escaping. Affects versions up to and including 5.0.3..	Patched by core rule	Y
CVE-2026-4306	The WP Job Portal plugin for WordPress is vulnerable to SQL Injection via the 'radius' parameter in all versions up t...	Vulnerability via the 'radius' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 2.4.8.	Patched by core rule	Y
CVE-2026-2412	The Quiz and Survey Master (QSM) plugin for WordPress is vulnerable to SQL Injection via the 'merged_question' parame...	Vulnerability via the 'merged_question' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 10.3.5..	Patched by core rule	Y
CVE-2026-33723	WWBN AVideo is an open source video platform.	An authenticated attacker can inject arbitrary SQL to extract sensitive data from any database table, including password hashes, API keys, and encryption salts. Commit 36dfae22059fbd66fd34bbc5568a838fc0efd66c contains a patch.	Patched by core rule	Y
CVE-2026-33651	WWBN AVideo is an open source video platform.	In versions up to and including 26.0, the `remindMe.json.php` endpoint passes `$_REQUEST['live_schedule_id']` through multiple functions without sanitization until it reaches `Scheduler_commands::getAllActiveOrToRepeat()`, which directly concatenates it into a SQL `LIKE` clause. Although intermediate functions (`new Live_schedule()`, `getUsers_idOrCompany()`) apply `intval()` internally, they do so on local copies within `ObjectYPT::getFromDb()`, leaving the original tainted variable unchanged.	Patched by core rule	Y
CVE-2026-33485	WWBN AVideo is an open source video platform.	The `$_POST['name']` parameter (stream key) is interpolated directly into SQL queries in two locations — `LiveTransmitionHistory::getLate	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		st()` and `LiveTransmition::keyExists()` — without parameterized binding or escaping. An unauthenticated attacker can exploit time-based blind SQL injection to extract all database contents including user password hashes, email addresses, and other sensitive data. Commit af59eade82de645b20183cc3d74467a7eac76549 contains a patch.		
CVE-2026-33352	WWBN AVideo is an open source video platform.	The parameter is not covered by any of the application's global input filters in `objects/security.php`. Version 26.0 contains a patch for the issue.	Patched by core rule	Y
CVE-2026-4574	SourceCodester Simple E-learning System — SQL Injection via firstname	This vulnerability affects unknown code of the component User Profile Update Handler. The manipulation of the argument firstName results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-4573	SourceCodester Simple E-learning System — SQL Injection	The manipulation of the argument post_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-4572	SourceCodester Sales and Inventory System — SQL Injection	Executing a manipulation of the argument searchtxt can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-4571	SourceCodester Sales and Inventory System — SQL Injection via searchtxt	Performing a manipulation of the argument searchtxt results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-4570	SourceCodester Sales and Inventory System — SQL Injection	Affected is an unknown function of the file /view_customers.php of the component HTTP POST Request Handler. Such manipulation of the argument searchtxt leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-4569	SourceCodester Sales and Inventory System — SQL Injection via searchtxt	This impacts an unknown function of the file /view_category.php of the component HTTP POST Request Handler. This manipulation of the argument searchtxt causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-4568	SourceCodester Sales and Inventory System — SQL Injection via sid	This affects an unknown function of the file /update_supplier.php of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component HTTP GET Request Handler. The manipulation of the argument sid results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used. Several companies clearly confirm that VulDB is the primary source for best vulnerability data.		
CVE-2026-2580	The WP Maps — Store Locator,Google Maps,OpenStreetMap,Mapbox,Listing,Directory & Filters plugin for WordPress is vuln...	Vulnerability via the 'orderby' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 4.9.1.	Patched by core rule	Y
CVE-2019-25581	i-doit CMDB 1.12 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary S...	Attackers can send GET requests with crafted SQL payloads in the objGroupID parameter to extract sensitive database information including usernames, database names, and version details.	Patched by core rule	Y
CVE-2019-25578	phpTransformer 2016.9 contains an SQL injection vulnerability that allows remote attackers to execute arbitrary SQL q...	Attackers can send crafted GET requests to GeneratePDF.php with SQL payloads in the idnews parameter to extract sensitive database information or manipulate queries.	Patched by core rule	Y
CVE-2019-25576	Kepler Wallpaper Script 1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute ...	Attackers can send GET requests to the category endpoint with URL-encoded SQL UNION statements to extract database information including usernames, database names, and MySQL version details.	Patched by core rule	Y
CVE-2019-25575	SimplePress CMS 1.0.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitr...	Attackers can send GET requests with crafted SQL payloads to extract sensitive database information including usernames, database names, and version details.	Patched by core rule	Y
CVE-2019-25573	Green CMS 2.x contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL qu...	Attackers can send GET requests to index.php with m=admin, c=posts, a=index parameters and inject SQL code in the cat parameter to manipulate database queries and extract sensitive information.	Patched by core rule	Y
CVE-2026-4087	The Pre* Party Resource Hints plugin for WordPress is vulnerable to SQL Injection via the 'hint_ids' parameter of the...	Vulnerability via the 'hint_ids' parameter of the pprh_update_hints AJAX action due to insufficient input sanitization or output escaping. Affects versions up to and including 1.8.20..	Patched by core rule	Y
CVE-2026-3334	The CMS Commander plugin for WordPress is vulnerable to SQL Injection via the 'or_blogname', 'or_blogdescription', an...	Vulnerability via the 'or_blogname', 'or_blogdescription', and 'or_admin_email' parameters due to insufficient input sanitization or output escaping. Affects versions up to and including 2.288..	Patched by core rule	Y
CVE-2026-2503	The ElementCamp plugin for WordPress is vulnerable to time-based SQL Injection via the 'meta_query[compare]' paramete...	Vulnerability via the 'meta_query[compare]' parameter in the 'tcg_select2_search_post' AJAX action due to insufficient input sanitization or output escaping. Affects versions up to and		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including 2.3.6..		
CVE-2026-2468	The Quentn WP plugin for WordPress is vulnerable to SQL Injection via the 'qntn_wp_access' cookie in all versions up ...	Vulnerability via the 'qntn_wp_access' cookie due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.12..	Patched by core rule	Y
CVE-2026-2279	The myLinksDump plugin for WordPress is vulnerable to SQL Injection via the 'sort_by' and 'sort_order' parameters in ...	Vulnerability via the 'sort_by' and 'sort_order' parameters due to insufficient input sanitization or output escaping. Affects versions up to and including 1.6.	Patched by core rule	Y
CVE-2026-1800	The Fonts Manager | Custom Fonts plugin for WordPress is vulnerable to time-based SQL Injection via the 'fmcfIdSelect...	Vulnerability via the 'fmcfIdSelectedFnt' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.	Patched by core rule	Y
CVE-2026-33134	WeGIA is a web manager for charitable institutions.	Versions 3.6.5 and below contain an authenticated SQL Injection vulnerability in the html/matPat/restaurar_produto.php endpoint. The vulnerability allows an authenticated attacker to inject arbitrary SQL commands via the id_produto GET parameter, leading to full database compromise. In the script /html/matPat/restaurar_produto.	Patched by core rule	Y
CVE-2026-33133	WeGIA is a web manager for charitable institutions.	In versions 3.6.5 and 3.6.6, the loadBackupDB() function imports SQL files from uploaded backup archives without any content validation. An attacker can craft a backup archive containing arbitrary SQL statements that create rogue administrator accounts, modify existing passwords, or execute any database operation. This was introduced in commit 370104c. This issue was patched in version 3.6.7.	Patched by core rule	Y
CVE-2026-4473	itsourcecode Online Doctor Appointment System — SQL Injection via appointment_id	This issue affects some unknown processing of the file /admin/appointment_action.php. The manipulation of the argument appointment_id results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-4472	itsourcecode Online Frozen Foods Ordering System — SQL Injection	The manipulation of the argument Supplier_Name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-4471	itsourcecode Online Frozen Foods Ordering System — SQL Injection	Executing a manipulation of the argument First_Name can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-4470	itsourcecode Online Frozen Foods Ordering System — SQL Injection via	Performing a manipulation of the argument product_name results in sql injection. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	product_name	possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.		
CVE-2026-4469	itsourcecode Online Frozen Foods Ordering System — SQL Injection	Affected by this vulnerability is an unknown functionality of the file /admin/admin_edit_menu_action.php. Such manipulation of the argument product_name leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-32813	Admidio is an open-source user management solution.	Versions 5.0.6 and below are vulnerable to arbitrary SQL Injection through the MyList configuration feature. The MyList configuration feature lets authenticated users define custom list column layouts, storing user-supplied column names, sort directions, and filter conditions in the adm_list_columns table via prepared statements.	Patched by core rule	Y
CVE-2026-32767	SiYuan is a personal knowledge management system.	Versions 3.6.0 and below contain an authorization bypass vulnerability in the /api/search/fullTextSearchBlock endpoint. When the method parameter is set to 2, the endpoint passes user-supplied input directly as a raw SQL statement to the underlying SQLite database without any authorization or read-only checks. This allows any authenticated user — including those with the Reader role — to execute arbitrary SQL statements (SELECT, DELETE, UPDATE, DROP TABLE, etc.	Patched by core rule	Y
CVE-2026-3658	The Appointment Booking Calendar ,Äî Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable t...	Vulnerability via the 'fields' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.6.10.0.	Patched by core rule	Y
CVE-2026-27413	Profile Builder Pro — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cozmoslabs Profile Builder Pro allows Blind SQL Injection.This issue affects Profile Builder Pro: from n/a through 3.13.9.	Patched by core rule	Y
CVE-2026-32321	ClipBucket v5 is an open source video sharing platform.	An authenticated time-based blind SQL injection vulnerability exists in ClipBucket prior to 5.5.3 #80 within the `actions/ajax.php` endpoint. Due to insufficient input sanitization of the `userid` parameter, an authenticated attacker can execute arbitrary SQL queries, leading to full database disclosure and potential administrative account takeover. Version 5.5.3 #80 fixes the issue.	Patched by core rule	Y
CVE-2026-32611	Glances is an open-source system cross-platform	The GHSA-x46r fix (commit 39161f0) addressed SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	monitoring tool.	injection in the TimescaleDB export module by converting all SQL operations to use parameterized queries and `psycopg.sql` composable objects. However, the DuckDB export module (`glances/exports/glances_duckdb/__init__.py`) was not included in this fix and contains the same class of vulnerability: table names and column names derived from monitoring statistics are directly interpolated into SQL statements via f-strings.		
CVE-2026-33058	Kanboard is project management software focused on Kanban methodology.	Versions prior to 1.2.51 have an authenticated SQL injection vulnerability. Attackers with the permission to add users to a project can leverage this vulnerability to dump the entirety of the kanboard database. Version 1.2.51 fixes the issue.	Patched by core rule	Y
CVE-2026-2579	The WowStore — Store Builder & Product Blocks for WooCommerce plugin for WordPress is vulnerable to SQL Injection via...	Vulnerability via the 'search' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 4.4.3.	Patched by core rule	Y
CVE-2025-69768	SQL Injection vulnerability in Chyrp v.2.5.2 and before allows a remote attacker to obtain sensitive information via ...	SQL Injection vulnerability in Chyrp v.2.5.2 and before allows a remote attacker to obtain sensitive information via the Admin.php component	Patched by core rule	Y
CVE-2026-4223	itsourcecode Payroll Management System — SQL Injection	This issue affects some unknown processing of the file /manage_employee.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-32628	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during cha...	In 1.11.1 and earlier, a SQL injection vulnerability in the built-in SQL Agent plugin allows any user who can invoke the agent to execute arbitrary SQL commands on connected databases. The getTableSchemaSql() method in all three database connectors (MySQL, PostgreSQL, MSSQL) constructs SQL queries using direct string concatenation of the table_name parameter without sanitization or parameterization.	Patched by core rule	Y
CVE-2015-20121	Next Click Ventures RealtyScript 4.0.2 contains SQL injection vulnerabilities that allow unauthenticated attackers to...	Attackers can exploit time-based blind SQL injection techniques to extract sensitive database information or cause denial of service through sleep-based payloads.	Patched by core rule	Y
CVE-2015-20120	Next Click Ventures RealtyScript 4.0.2 contains multiple time-based blind SQL injection vulnerabilities that allow un...	Attackers can craft requests with time-delay payloads to infer database contents character by character based on response timing differences.	Patched by core rule	Y
CVE-2026-32459	UpsellWP — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Command ('SQL Injection') vulnerability in flycart UpsellWP checkout-upsell-and-order-bumps allows Blind SQL Injection.This issue affects UpsellWP: from n/a through <= 2.2.4.		
CVE-2026-32458	WOLF — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 WOLF bulk-editor allows Blind SQL Injection.This issue affects WOLF: from n/a through <= 1.0.8.7.	Patched by core rule	Y
CVE-2026-32433	CP Contact Form with Paypal — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in codepeople CP Contact Form with Paypal cp-contact-form-with-paypal allows Blind SQL Injection.This issue affects CP Contact Form with Paypal: from n/a through <= 1.3.61.	Patched by core rule	Y
CVE-2026-32422	WP EasyCart — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in levelfourdevelopment WP EasyCart wp-easycart allows Blind SQL Injection.This issue affects WP EasyCart: from n/a through <= 5.8.13.	Patched by core rule	Y
CVE-2026-32418	Meow Gallery — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jordy Meow Meow Gallery meow-gallery allows Blind SQL Injection.This issue affects Meow Gallery: from n/a through <= 5.4.4.	Patched by core rule	Y
CVE-2026-32399	Media LIbrary Assistant — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David Lingren Media LIbrary Assistant media-library-assistant allows Blind SQL Injection.This issue affects Media LIbrary Assistant: from n/a through <= 3.32.	Patched by core rule	Y
CVE-2026-32368	Geo to Lat — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in delphiknight Geo to Lat geo-to-lat allows Blind SQL Injection.This issue affects Geo to Lat: from n/a through <= 1.0.19.	Patched by core rule	Y
CVE-2026-32366	Collapsing Categories — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in robfelty Collapsing Categories collapsing-categories allows Blind SQL Injection.This issue affects Collapsing Categories: from n/a through <= 3.0.9.	Patched by core rule	Y
CVE-2026-32365	Collapsing Archives — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability in robfelty Collapsing Archives collapsing-archives allows Blind SQL Injection.This issue affects Collapsing Archives: from n/a through <= 3.0.7.		
CVE-2026-32358	Booking Calendar — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpdevelop Booking Calendar booking allows Blind SQL Injection.This issue affects Booking Calendar: from n/a through <= 10.14.15.	Patched by core rule	Y
CVE-2026-32306	OneUptime is a solution for monitoring and managing online services.	Prior to 10.0.23, the telemetry aggregation API accepts user-controlled aggregationType, aggregateColumnName, and aggregationTimestampColumnName parameters and interpolates them directly into ClickHouse SQL queries via the .append() method (documented as "trusted SQL"). There is no allowlist, no parameterized query binding, and no input validation.	Patched by core rule	Y
CVE-2026-31922	Fox LMS — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ays Pro Fox LMS fox-lms allows Blind SQL Injection.This issue affects Fox LMS: from n/a through <= 1.0.6.3.	Patched by core rule	Y
CVE-2026-31917	WP ERP — SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP ERP erp allows SQL Injection.This issue affects WP ERP: from n/a through <= 1.16.10.	Patched by core rule	Y
CVE-2026-32137	Dataease is an open source data visualization analysis tool.	Prior to 2.10.20, The table parameter for /de2api/datasource/previewData is directly concatenated into the SQL statement without any filtering or parameterization. Since tableName is a user-controllable string, attackers can inject malicious SQL statements by constructing malicious table names. This vulnerability is fixed in 2.10.20.	Patched by core rule	Y
CVE-2026-26794	GL-iNet GL-AR300M16 v4.3.11 was discovered to contain a SQL injection vulnerability via the add_group() function.	This vulnerability allows attackers to execute arbitrary SQL database operations via a crafted HTTP request.	Patched by core rule	Y
CVE-2019-25543	Netartmedia Real Estate Portal 5.0 contains an SQL injection vulnerability that allows unauthenticated attackers to m...	Attackers can submit POST requests to index.php with malicious SQL payloads in the page field to bypass authentication, extract sensitive data, or modify database contents.	Patched by core rule	Y
CVE-2019-25542	Netartmedia Real Estate Portal 5.0 contains a SQL injection vulnerability that allows unauthenticated attackers to ma...	Attackers can send POST requests to index.php with malicious payloads in the user_email field to bypass authentication, extract sensitive	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		data, or modify database contents.		
CVE-2019-25541	Netartmedia PHP Mall 4.1 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to mani...	Attackers can inject time-based blind SQL payloads via the 'id' parameter in index.php or the 'Email' parameter in loginaction.php to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25540	Netartmedia PHP Mall 4.1 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to mani...	Attackers can craft malicious requests with SQL payloads to extract sensitive database information including user credentials and system data.	Patched by core rule	Y
CVE-2019-25539	202CMS v10 beta contains a blind SQL injection vulnerability that allows unauthenticated attackers to manipulate data...	Attackers can send POST requests to index.php with crafted SQL payloads using time-based blind injection techniques to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25538	202CMS v10 beta contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database ...	Attackers can send crafted requests with malicious SQL statements in the log_user field to extract sensitive database information or modify database contents.	Patched by core rule	Y
CVE-2019-25537	Netartmedia Event Portal 2.0 contains a time-based blind SQL injection vulnerability that allows unauthenticated atta...	Attackers can send POST requests to loginaction.php with malicious SQL payloads in the Email field to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25536	Netartmedia PHP Real Estate Agency 4.0 contains an SQL injection vulnerability that allows unauthenticated attackers ...	Attackers can send POST requests to index.php with crafted SQL payloads in the features[] parameter to extract sensitive database information or manipulate database queries.	Patched by core rule	Y
CVE-2019-25535	Netartmedia PHP Dating Site contains a SQL injection vulnerability that allows unauthenticated attackers to manipulat...	Attackers can send POST requests to loginaction.php with time-based SQL injection payloads in the Email field to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25534	Netartmedia PHP Car Dealer contains an SQL injection vulnerability that allows unauthenticated attackers to execute a...	Attackers can submit POST requests to index.php with crafted SQL payloads in the features[] parameter to extract sensitive database information or manipulate database queries.	Patched by core rule	Y
CVE-2019-25533	Netartmedia PHP Business Directory 4.2 contains an SQL injection vulnerability that allows unauthenticated attackers ...	Attackers can send POST requests to the loginaction.php endpoint with crafted SQL payloads in the Email field to extract sensitive database information or bypass authentication.	Patched by core rule	Y
CVE-2019-25532	Netartmedia Jobs Portal 6.1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipula...	Attackers can send POST requests to loginaction.php with crafted SQL payloads in the Email field to extract sensitive database information or bypass authentication.	Patched by core rule	Y
CVE-2019-25531	Netartmedia Deals Portal contains an SQL injection vulnerability in the Email parameter of loginaction.php that allow...	Attackers can submit crafted SQL payloads through POST requests to extract sensitive information or bypass authentication mechanisms.	Patched by core rule	Y
CVE-2019-25530	uHotelBooking System contains an SQL injection vulnerability that allows	Attackers can send crafted requests to index.php with malicious system_page values	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	unauthenticated attackers to manipulate data...	using time-based blind SQL injection techniques to extract sensitive database information.		
CVE-2019-25529	Placeto CMS Alpha rv.4 contains an SQL injection vulnerability that allows authenticated attackers to manipulate data...	Attackers can send GET requests to the admin/edit.php endpoint with malicious 'page' values using boolean-based blind, time-based blind, or union-based techniques to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25528	Inout EasyRooms Ultimate Edition v1.0 contains an SQL injection vulnerability that allows unauthenticated attackers t...	Attackers can send POST requests to the search/searchdetailed endpoint with malicious SQL payloads to extract sensitive data or modify database contents.	Patched by core rule	Y
CVE-2019-25527	Inout EasyRooms Ultimate Edition v1.0 contains an SQL injection vulnerability that allows unauthenticated attackers t...	Attackers can send POST requests to the search/searchdetailed endpoint with malicious SQL payloads to bypass authentication, extract sensitive data, or modify database contents.	Patched by core rule	Y
CVE-2019-25526	Inout EasyRooms Ultimate Edition v1.0 contains an SQL injection vulnerability that allows unauthenticated attackers t...	Attackers can send POST requests to the search/searchdetailed endpoint with malicious SQL payloads in the location field to extract sensitive data or modify database contents.	Patched by core rule	Y
CVE-2019-25525	Inout EasyRooms Ultimate Edition v1.0 contains an SQL injection vulnerability that allows unauthenticated attackers t...	Attackers can send POST requests to the search/rentals endpoint with malicious SQL payloads to bypass authentication, extract sensitive data, or modify database contents.	Patched by core rule	Y
CVE-2019-25524	XooGallery Latest contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send GET requests to results.php with malicious 'p' values to bypass authentication, extract sensitive data, or modify database contents.	Patched by core rule	Y
CVE-2019-25523	XooGallery Latest contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send GET requests to cat.php with malicious cat_id values to bypass authentication, extract sensitive data, or modify database contents.	Patched by core rule	Y
CVE-2019-25522	XooGallery Latest contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to manipulate ...	Attackers can send GET requests to photo.php with malicious photo_id values to extract sensitive data, bypass authentication, or modify database contents.	Patched by core rule	Y
CVE-2019-25521	XooGallery Latest contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send GET requests to gal.php with malicious gal_id values to extract sensitive database information or modify database contents.	Patched by core rule	Y
CVE-2019-25520	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an authentication bypass vulnerability in the administration panel...	Attackers can submit SQL injection payloads in the username and password fields of the admingiris.php login form to bypass authentication and access the administrative interface.	Patched by core rule	Y
CVE-2019-25519	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an SQL injection vulnerability that allows attackers to	Attackers can send POST requests to uyelik.php with crafted payloads in the option parameter to execute time-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	manipulate...	based SQL injection attacks and extract sensitive database information.		
CVE-2019-25518	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an SQL injection vulnerability that allows unauthenticated attacke...	Attackers can send POST requests to arama.php with malicious SQL payloads in the poll parameter to extract sensitive data or modify database contents.	Patched by core rule	Y
CVE-2019-25517	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an SQL injection vulnerability that allows unauthenticated attacke...	Attackers can send requests to haberarsiv.php with malicious cid values using UNION-based injection to extract sensitive database information or modify database contents.	Patched by core rule	Y
CVE-2019-25516	Jettweb PHP Hazir Haber Sitesi Scripti V1 contains an SQL injection vulnerability that allows unauthenticated attacke...	Attackers can send GET requests to gallery.php with malicious gallery_id values using UNION-based SQL injection to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25515	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an authentication bypass vulnerability in the login.php administra...	Attackers can bypass authentication by submitting equals signs and 'or' operators as username and password parameters to access the administration panel without valid credentials.	Patched by core rule	Y
CVE-2019-25514	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an SQL injection vulnerability that allows attackers to inject mal...	Attackers can manipulate the kelime parameter with UNION-based SQL injection payloads to extract sensitive data from the database or bypass authentication controls.	Patched by core rule	Y
CVE-2019-25513	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an SQL injection vulnerability that allows unauthenticated attacke...	Attackers can send GET requests to datagetir.php with malicious 'q' values using time-based blind SQL injection techniques to extract sensitive database information or bypass authentication.	Patched by core rule	Y
CVE-2019-25512	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an SQL injection vulnerability that allows attackers to inject mal...	Attackers can manipulate the kelime parameter with UNION-based SQL injection payloads to extract sensitive database information or modify database contents.	Patched by core rule	Y
CVE-2019-25511	Jettweb PHP Hazir Haber Sitesi Scripti V3 contains an SQL injection vulnerability that allows unauthenticated attacke...	Attackers can send GET requests to fonksiyonlar.php with malicious videoid values using UNION-based injection to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25510	Jettweb PHP Hazir Haber Sitesi Scripti V2 contains an authentication bypass vulnerability in the administration panel...	Attackers can submit SQL injection payloads in the username and password fields of the admingiris.php login form to bypass authentication and access the administrative interface.	Patched by core rule	Y
CVE-2019-25509	XooDigital Latest contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send GET requests to results.php with malicious 'p' values to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25508	Jettweb Php Hazir Ilan Sitesi Scripti V2 contains an SQL injection vulnerability that allows unauthenticated attacker...	Attackers can send GET requests to the katgetir.php endpoint with malicious 'kat' values to extract sensitive database information.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2019-25488	Jettweb Hazir Rent A Car Scripti V4 contains multiple SQL injection vulnerabilities in the admin panel that allow una...	Attackers can inject SQL code into the 'tur', 'id', and 'ozellikdil' parameters of the admin/index.php endpoint to extract sensitive database information or cause denial of service.	Patched by core rule	Y
CVE-2019-25482	Jettweb PHP Hazir Rent A Car Sitesi Scripti V2 contains an SQL injection vulnerability that allows unauthenticated at...	Attackers can send POST requests to the endpoint with malicious SQL payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25481	iScripts ReserveLogic contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate dat...	Attackers can send POST requests to the search endpoint with crafted SQL payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25479	Inout RealEstate contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database...	Attackers can send POST requests to the agents/agentlistdetails endpoint with malicious SQL payloads in the city parameter to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25473	Clinic Pro contains a SQL injection vulnerability that allows authenticated attackers to manipulate database queries ...	Attackers can send POST requests to the monthly_expense_overview endpoint with crafted month values using boolean-based blind, time-based blind, or error-based SQL injection techniques to extract sensitive database information.	Patched by core rule	Y
CVE-2026-4014	itsourcecode Cafe Reservation System — SQL Injection via username	Performing a manipulation of the argument Username results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-3981	itsourcecode Online Doctor Appointment System — SQL Injection via id	Affected is an unknown function of the file /admin/doctor_action.php. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3980	itsourcecode Online Doctor Appointment System — SQL Injection	Such manipulation of the argument patient_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-3657	The My Sticky Bar plugin for WordPress is vulnerable to SQL injection via the `stickymenu_contact_lead_form` AJAX act...	Vulnerability via the `stickymenu_contact_lead_form` AJAX action due to insufficient input sanitization or output escaping. Affects versions up to and including 2.8.6..	Patched by core rule	Y
CVE-2026-32127	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.1, OpenEMR contains a SQL injection vulnerability in the ajax graphs library that can be exploited by authenticated attackers. The vulnerability exists due to insufficient input validation in the ajax graphs library. This vulnerability is fixed in 8.0.0.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-31896	WeGIA is a web manager for charitable institutions.	Prior to version 3.6.6, a critical SQL injection vulnerability exists in the WeGIA application. The remover_produto_ocultar.php script uses extract($_REQUEST) to populate local variables and then directly concatenates these variables into a SQL query executed via PDO::query. This allows an authenticated (or auth-bypassed) attacker to execute arbitrary SQL commands.	Patched by core rule	Y
CVE-2026-31895	WeGIA is a web manager for charitable institutions.	Prior to version 3.6.6, WeGIA (Web gerenciador para instituiVßVµes assistenciais) contains a SQL injection vulnerability in html/matPat/restaurar_produto.php. The id_produto parameter from $_GET is directly interpolated into SQL queries without parameterization or sanitization. This vulnerability is fixed in 3.6.6.	Patched by core rule	Y
CVE-2019-25486	Varient 1.6.1 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database qu...	Attackers can submit POST requests with crafted SQL payloads in the user_id field to bypass authentication and extract sensitive database information.	Patched by core rule	Y
CVE-2026-3496	The JetBooking plugin for WordPress is vulnerable to SQL Injection via the 'check_in_date' parameter in all versions ...	Vulnerability via the 'check_in_date' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 4.0.3..	Patched by core rule	Y
CVE-2026-3944	itsourcecode University Management System — SQL Injection via name	This vulnerability affects unknown code of the file /att_add.php. This manipulation of the argument Name causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-1708	The Appointment Booking Calendar ‚Äî Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable t...	This is due to the `db_where_conditions` method in the `TD_DB_Model` class failing to prevent the `append_where_sql` parameter from being passed through JSON request bodies, while only checking for its presence in the `$_REQUEST` superglobal.	Patched by core rule	Y
CVE-2026-3222	The WP Maps plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'location_id' parameter in a...	Vulnerability via the 'location_id' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 4.9.1..	Patched by core rule	Y
CVE-2026-2413	The Ally — Web Accessibility & Usability plugin for WordPress is vulnerable to SQL Injection via the URL path in all ...	Vulnerability via the URL path due to insufficient input sanitization or output escaping. Affects versions up to and including 4.0.3..	Patched by core rule	Y
CVE-2026-30951	Sequelize is a Node.js ORM tool.	Prior to 6.37.8, there is SQL injection via unescaped cast type in JSON/JSONB where clause processing. The _traverseJSON() function splits JSON path keys on :: to extract a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cast type, which is interpolated raw into CAST(... AS <type>) SQL. An attacker who controls JSON object keys can inject arbitrary SQL and exfiltrate data from any table. This vulnerability is fixed in 6.37.8.		
CVE-2026-29174	Craft Commerce is an ecommerce platform for Craft CMS.	Prior to 5.5.3, Craft Commerce is vulnerable to SQL Injection in the inventory levels table data endpoint. The sort[0][direction] and sort[0][sortField] parameters are concatenated directly into an addOrderBy() clause without any validation or sanitization. An authenticated attacker with access to the Commerce Inventory section can inject arbitrary SQL queries, potentially leading to a full database compromise. This vulnerability is fixed in 5.5.3.	Patched by core rule	Y
CVE-2026-29172	Craft Commerce is an ecommerce platform for Craft CMS.	Prior to 4.10.2 and 5.5.3, Craft Commerce is vulnerable to SQL Injection in the purchasables table endpoint. The sort parameter is split by | and the first part (column name) is passed directly as an array key to orderBy() without whitelist validation. Yii2's query builder does NOT escape array keys, allowing an authenticated attacker to inject arbitrary SQL into the ORDER BY clause. This vulnerability is fixed in 4.10.2 and 5.5.3.	Patched by core rule	Y
CVE-2026-30930	Glances is an open-source system cross-platform monitoring tool.	Prior to 4.5.1, The TimescaleDB export module constructs SQL queries using string concatenation with unsanitized system monitoring data. The normalize() method wraps string values in single quotes but does not escape embedded single quotes, making SQL injection trivial via attacker-controlled data such as process names, filesystem mount points, network interface names, or container names. This vulnerability is fixed in 4.5.1.	Patched by core rule	Y
CVE-2026-3806	SourceCodester/janobe Resort Reservation System — SQL Injection via q	This manipulation of the argument q causes sql injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-3798	A vulnerability was detected in Comfast CF-AC100 2.6.0.8.	This affects the function sub_44AC14 of the file /cgi-bin/mbox-config?method=SET&section=ping_config of the component Request Path Handler. The manipulation results in command injection. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3793	SourceCodester Sales and Inventory System — SQL	This vulnerability affects unknown code of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Injection via sellid	sales_invoice1.php of the component GET Parameter Handler. This manipulation of the argument sellid causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.		
CVE-2026-3792	SourceCodester Sales and Inventory System — SQL Injection via purchaseid	This affects an unknown part of the file purchase_invoice.php of the component GET Parameter Handler. The manipulation of the argument purchaseid results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3791	SourceCodester Sales and Inventory System — SQL Injection	The manipulation of the argument searchtxt leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-3790	SourceCodester Sales and Inventory System — SQL Injection	Executing a manipulation of the argument stock_name1 can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-3786	EasyCMS up to — SQL Injection via _order	The manipulation of the argument _order results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3785	EasyCMS up to — SQL Injection	The affected element is an unknown function of the file /RbacnodeAction.class.php of the component Request Parameter Handler. The manipulation of the argument _order leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3771	SourceCodester/janobe Resort Reservation System — SQL Injection	Such manipulation of the argument q leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-3767	itsourcecode sanitize or validate this input — SQL Injection	Affected is an unknown function of the file /admin/teacher-attendance.php. Executing a manipulation of the argument teacher_id can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-3765	itsourcecode University Management System — SQL Injection	This affects an unknown function of the file /att_single_view.php. Such manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		dt leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.		
CVE-2026-3760	itsourcecode University Management System — SQL Injection via seme	This vulnerability affects unknown code of the file /view_result.php. Performing a manipulation of the argument seme results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-3759	projectworlds Online Art Gallery Shop — SQL Injection	Such manipulation of the argument reach_nm leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-3758	projectworlds Online Art Gallery Shop — SQL Injection via info	This manipulation of the argument Info causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-3757	projectworlds Online Art Gallery Shop — SQL Injection via fnm	The manipulation of the argument fnm results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-3756	SourceCodester Sales and Inventory System up to — SQL Injection	Affected is an unknown function of the file /check_item_details.php. The manipulation of the argument stock_name1 leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-3755	SourceCodester Sales and Inventory System — SQL Injection	This impacts an unknown function of the file /check_customer_details.php of the component POST Handler. Executing a manipulation of the argument stock_name1 can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-3754	SourceCodester Sales and Inventory System — SQL Injection via cost	This affects an unknown function of the file /add_stock.php. Performing a manipulation of the argument cost results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3753	SourceCodester Sales and Inventory System up to — SQL Injection	Such manipulation of the argument sid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-3752	SourceCodester Employee Task Management System up to — SQL Injection via date	This manipulation of the argument Date causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-3751	SourceCodester Employee Task Management System — SQL Injection via date	Impacted is an unknown function of the file /daily-attendance-report.php of the component GET Parameter Handler. The manipulation of the argument Date results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-3747	itsourcecode University Management System — SQL Injection	Affected by this issue is some unknown functionality of the file /add_result.php. Such manipulation of the argument subject leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-3746	SourceCodester Simple Responsive Tourism Website — SQL Injection via username	Affected by this vulnerability is an unknown functionality of the file /tourism/classes/Login.php?f=login of the component Login. This manipulation of the argument Username causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-3745	code-projects Student Web Portal — SQL Injection via user	Affected is an unknown function of the file profile.php. The manipulation of the argument User results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3744	code-projects Student Web Portal — SQL Injection	The manipulation of the argument reg_passwd leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-3740	itsourcecode University Management System — SQL Injection via admin_search_student	This manipulation of the argument admin_search_student causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-3736	code-projects Simple Flight Ticket Booking System — SQL Injection via from	Affected by this issue is some unknown functionality of the file SearchResultRoundtrip.php. Performing a manipulation of the argument from results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3735	code-projects Simple Flight Ticket Booking System — SQL Injection	Such manipulation of the argument from leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-3730	itsourcecode Free Hotel Reservation System — SQL Injection	Performing a manipulation of the argument amen_id/rmtype_id results in sql injection. The attack is possible to be carried out remotely. The exploit has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		released to the public and may be used for attacks.		
CVE-2026-3723	code-projects Simple Flight Ticket Booking System — SQL Injection via flightno	The manipulation of the argument flightno results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-3711	code-projects Simple Flight Ticket Booking System — SQL Injection	Affected is an unknown function of the file /Adminupdate.php. The manipulation of the argument flightno/airplaneid/departure/dtime/arrival/atime/ec/ep/bc/bp results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-3710	code-projects Simple Flight Ticket Booking System — SQL Injection	The manipulation of the argument flightno/airplaneid/departure/dtime/arrival/atime/ec/ep/bc/bp leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-3709	code-projects Simple Flight Ticket Booking System — SQL Injection	Executing a manipulation of the argument Username can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-3708	code-projects Simple Flight Ticket Booking System — SQL Injection via username	Performing a manipulation of the argument Username results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-3705	code-projects Simple Flight Ticket Booking System — SQL Injection via flightno	This issue affects some unknown processing of the file /Adminsearch.php. The manipulation of the argument flightno results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3704	A vulnerability has been found in Wavlink NU516U1 251208.	The manipulation leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	Patched by core rule	Y
CVE-2026-30860	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval.	Prior to version 0.2.12, a remote code execution (RCE) vulnerability exists in the application's database query functionality. The validation system fails to recursively inspect child nodes within PostgreSQL array expressions and row expressions, allowing	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers to bypass SQL injection protections.		
CVE-2026-30852	Caddy is an extensible server platform that uses TLS by default.	From version 2.7.5 to before version 2.11.2, the vars_regexp matcher in vars.go:337 double-expands user-controlled input through the Caddy replacer. When vars_regexp matches against a placeholder like {http.request.header.X-Input}, the header value gets resolved once (expected), then passed through repl.ReplaceAll() again (the bug). This means an attacker can put {env.DATABASE_URL} or {file.	Patched by core rule	Y
CVE-2026-3662	A vulnerability has been found in Wavlink WL-NU516U1 240425.	Such manipulation of the argument Pr_mode leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2026-3661	A flaw has been found in Wavlink WL-NU516U1 240425.	This manipulation of the argument model causes command injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2026-2429	The Community Events plugin for WordPress is vulnerable to SQL Injection via the 'ce_venue_name' CSV field in the `on...	Vulnerability via the 'ce_venue_name' CSV field in the `on_save_changes_venues` function due to insufficient input sanitization or output escaping. Affects versions up to and including 1.5.8..	Patched by core rule	Y
CVE-2025-14353	The ZIP Code Based Content Protection plugin for WordPress is vulnerable to SQL Injection in all versions up to, and ...	This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2018-25199	OOP CMS BLOG 1.0 contains SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL...	Attackers can inject SQL commands via the search parameter in search.php, pageid parameter in page.php, and id parameter in posts.php to extract database information including table names, schema names, and database credentials.	Patched by core rule	Y
CVE-2018-25197	PlayJoom 0.10.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQ...	Attackers can send GET requests to index.php with option=com_playjoom&view=genre&catid=[SQL] to extract sensitive database information including usernames, databases, and version details.	Patched by core rule	Y
CVE-2018-25196	ServerZilla 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database ...	Attackers can send POST requests to reset.php with malicious email values containing SQL operators to bypass authentication and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		extract sensitive database information.		
CVE-2018-25194	Nominas 0.27 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL q...	Attackers can send POST requests to the login/checklogin.php endpoint with crafted UNION-based SQL injection payloads to extract database information including usernames, database names, and version details.	Patched by core rule	Y
CVE-2018-25192	GPS Tracking System 2.12 contains an SQL injection vulnerability that allows unauthenticated attackers to bypass auth...	Attackers can submit crafted POST requests to the login.php endpoint with SQL injection payloads in the username field to gain unauthorized access without valid credentials.	Patched by core rule	Y
CVE-2018-25191	Facturation System 1.0 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitra...	Attackers can send POST requests to the editar_producto.php endpoint with crafted SQL payloads in the mod_id parameter to extract sensitive database information including usernames, database names, and version details.	Patched by core rule	Y
CVE-2018-25189	Data Center Audit 2.6.2 contains an SQL injection vulnerability in the username parameter of dca_login.php that allow...	Attackers can submit crafted SQL payloads through POST requests to extract sensitive database information including usernames, database names, and version details.	Patched by core rule	Y
CVE-2018-25188	Webiness Inventory 2.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbit...	Attackers can send POST requests to the WsModelGrid.php endpoint with crafted SQL payloads to extract sensitive database information including usernames, databases, and version details.	Patched by core rule	Y
CVE-2018-25187	Tina4 Stack 1.0.3 contains multiple vulnerabilities allowing unauthenticated attackers to access sensitive database f...	Attackers can directly request the kim.db database file to retrieve user credentials and password hashes, or inject SQL code through the menu endpoint to manipulate database queries.	Patched by core rule	Y
CVE-2018-25182	Silurus Classifieds Script 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execu...	Attackers can send GET requests to wcategory.php with crafted SQL payloads in the ID parameter to extract database table names and sensitive information from the database.	Patched by core rule	Y
CVE-2018-25180	Maitra 1.7.2 contains an sql injection vulnerability that allows authenticated attackers to execute arbitrary SQL que...	Attackers can also download the SQLite database file directly from the application directory to extract sensitive mail tracking data and credentials.	Patched by core rule	Y
CVE-2018-25179	Gumbo CMS 0.99 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL...	Attackers can send POST requests to the settings endpoint with crafted SQL payloads in the language parameter to extract sensitive database information including usernames, databases, and version details.	Patched by core rule	Y
CVE-2018-25175	Alienor Web Libre 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitr...	Attackers can submit crafted POST requests to index.php with SQL injection payloads in the identifiant field to extract sensitive database information including usernames, databases,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and version details.		
CVE-2018-25173	Rmedia SMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to extract database info...	Attackers can send GET requests to editgrp.php with malicious gid values using EXTRACTVALUE and CONCAT functions to retrieve schema names and sensitive database data.	Patched by core rule	Y
CVE-2018-25172	Pedidos 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL qu...	Attackers can send GET requests to the ajax/load_proveedores.php endpoint with crafted SQL payloads to extract sensitive database information including schema names and table structures.	Patched by core rule	Y
CVE-2018-25167	Net-Billetterie 2.9 contains an SQL injection vulnerability in the login parameter of login.inc.php that allows unaut...	Attackers can submit malicious SQL code through the login POST parameter to extract database information including usernames, passwords, and system credentials.	Patched by core rule	Y
CVE-2018-25166	Meneame English Pligg 5.8 contains an SQL injection vulnerability that allows unauthenticated attackers to execute ar...	Attackers can send GET requests to index.php with crafted SQL payloads in the search parameter to extract sensitive database information including usernames, database names, and version details.	Patched by core rule	Y
CVE-2018-25165	Galaxy Forces MMORPG 0.5.8 contains an SQL injection vulnerability that allows authenticated attackers to execute arb...	Attackers can send POST requests to ads.php with crafted SQL payloads in the type parameter to extract sensitive database information including usernames, databases, and version details.	Patched by core rule	Y
CVE-2018-25163	BitZoom 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL qu...	Attackers can submit crafted POST requests with SQL UNION statements to extract database schema information and table contents from the application database.	Patched by core rule	Y
CVE-2018-25161	Warranty Tracking System 11.06.3 contains an SQL injection vulnerability that allows attackers to execute arbitrary S...	Attackers can submit crafted SQL statements using UNION SELECT to extract sensitive database information including usernames, database names, and version details.	Patched by core rule	Y
CVE-2026-29073	SiYuan is a personal knowledge management system.	Prior to version 3.6.0, the /api/query/sql lets a user run sql directly, but it only checks basic auth, not admin rights, any logged-in user, even readers, can run any sql query on the database. This issue has been patched in version 3.6.0.	Patched by core rule	Y
CVE-2026-27005	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to creat...	Prior to version 4.8.3, an unauthenticated attacker can inject arbitrary SQL into queries executed against databases connected to Chartbrew (MySQL, PostgreSQL). This allows reading, modifying, or deleting data in those databases depending on the database user's privileges. This issue has been patched in version 4.8.3.	Patched by core rule	Y
CVE-2026-3612	A vulnerability was determined in Wavlink WL-NU516U1 V240425.	This affects the function sub_405AF4 of the file /cgi-bin/adm.cgi of the component	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		OTA Online Upgrade. This manipulation of the argument firmware_url causes command injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.		
CVE-2026-28443	OpenReplay is a self-hosted session replay suite.	Prior to version 1.20.0, the POST /{projectId}/cards/search endpoint has a SQL injection in the sort.field parameter. This issue has been patched in version 1.20.0.	Patched by core rule	Y
CVE-2026-2893	The Page and Post Clone plugin for WordPress is vulnerable to SQL Injection via the 'meta_key' parameter in the conte...	Vulnerability via the 'meta_key' parameter in the content_clone() function due to insufficient input sanitization or output escaping. Affects versions up to and including 6.3..	Patched by core rule	Y
CVE-2026-28115	WP Attractive Donations System - Easy Stripe & Paypal donations — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in loopus WP Attractive Donations System - Easy Stripe & Paypal donations WP_AttractiveDonationsSystem allows Blind SQL Injection.This issue affects WP Attractive Donations System - Easy Stripe & Paypal donations: from n/a through <= 1.25.	Patched by core rule	Y
CVE-2026-27428	Eagle Booking — SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eagle-Themes Eagle Booking eagle-booking allows SQL Injection.This issue affects Eagle Booking: from n/a through <= 1.3.4.3.	Patched by core rule	Y
CVE-2026-27373	Tablesome — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Essekia Tablesome tablesome allows Blind SQL Injection.This issue affects Tablesome: from n/a through <= 1.2.3.	Patched by core rule	Y
CVE-2025-69338	Riode Core — Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in don-themes Riode Core riode-core allows Blind SQL Injection.This issue affects Riode Core: from n/a through <= 1.6.26.	Patched by core rule	Y
CVE-2026-3523	The Apocalypse Meow plugin for WordPress is vulnerable to SQL Injection via the 'type' parameter in all versions up t...	Vulnerability via the 'type' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 22.1.0..	Patched by core rule	Y
CVE-2019-25507	Ashop Shopping Cart Software contains an SQL injection vulnerability that allows unauthenticated attackers to manipul...	Attackers can send GET requests to index.php with malicious 'shop' values using UNION-based SQL injection to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25506	FreeSMS 2.1.2 contains a boolean-based blind SQL injection vulnerability in the	Attackers can exploit the vulnerable password parameter in requests to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	password parameter that allows unauth...	/pages/crc_handler.php?method=login to authenticate as any known user and subsequently modify their password via the profile update function.		
CVE-2019-25505	Tradebox 5.4 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queri...	Attackers can send POST requests to the monthly_deposit endpoint with malicious symbol values using boolean-based blind, time-based blind, error-based, or union-based SQL injection techniques to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25504	NCrypted Jobgator contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send POST requests to the agents Find-Jobs endpoint with malicious experience values to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25503	PHPads 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL que...	Attackers can submit crafted bannerID values using SQL comment syntax and functions like extractvalue to extract sensitive database information such as the current database name.	Patched by core rule	Y
CVE-2019-25501	Simple Job Script contains an SQL injection vulnerability that allows attackers to manipulate database queries by inj...	Attackers can send POST requests to delete_application_ajax.php with crafted payloads to extract sensitive data, bypass authentication, or modify database contents.	Patched by core rule	Y
CVE-2019-25500	Simple Job Script contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send POST requests to the register-recruiters endpoint with time-based SQL injection payloads to extract sensitive data or modify database contents.	Patched by core rule	Y
CVE-2019-25499	Simple Job Script contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send POST requests to get_job_applications_ajax.php with malicious job_id values to bypass authentication, extract sensitive data, or modify database contents.	Patched by core rule	Y
CVE-2019-25498	Simple Job Script contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send POST requests to the searched endpoint with malicious SQL payloads to bypass authentication and extract sensitive database information.	Patched by core rule	Y
CVE-2025-66944	SQL Injection vulnerability in vran-dev databaseir v.1.0.7 and before allows a remote attacker to execute arbitrary c...	SQL Injection vulnerability in vran-dev databaseir v.1.0.7 and before allows a remote attacker to execute arbitrary code via the query parameter in the search API endpoint	Patched by core rule	Y
CVE-2025-66678	An issue in the HwRwDrv.sys component of Nil Hardware Editor Hardware Read & Write Utility v1.25.11.26 and earlier al...	An issue in the HwRwDrv.sys component of Nil Hardware Editor Hardware Read & Write Utility v1.25.11.26 and earlier allows attackers to execute arbitrary read and write operations via a crafted request.	Patched by core rule	Y
CVE-2023-7337	The JS Help Desk — AI-Powered Support & Ticketing System plugin for WordPress is vulnerable to SQL Injection via the ...	This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sensitive information from the database.		
CVE-2026-2363	The WP-Members Membership Plugin plugin for WordPress is vulnerable to SQL Injection via the 'order_by' attribute of ...	Vulnerability via the 'order_by' attribute of the [wpmem_user_membership_posts] shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 3.5.5.1..	Patched by core rule	Y
CVE-2026-1651	The Email Subscribers by Icegram Express plugin for WordPress is vulnerable to SQL Injection via the 'workflow_ids' p...	Vulnerability via the 'workflow_ids' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 5.9.16.	Patched by core rule	Y
CVE-2026-3487	itsourcecode College Management System — SQL Injection via course_code	This issue affects some unknown processing of the file /admin/class-result.php. Performing a manipulation of the argument course_code results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3486	itsourcecode College Management System — SQL Injection	Such manipulation of the argument roll_no leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-26892	Sourcecodester Logistic Hub Parcel's Management System v1.0 is vulnerable to SQL Injection in /manage_carrier.php.	Sourcecodester Logistic Hub Parcel's Management System v1.0 is vulnerable to SQL Injection in /manage_carrier.php.	Patched by core rule	Y
CVE-2026-26891	Sourcecodester Logistic Hub Parcel's Management System v1.0 is vulnerable to SQL Injection in /manage_parcel_type.php.	Sourcecodester Logistic Hub Parcel's Management System v1.0 is vulnerable to SQL Injection in /manage_parcel_type.php.	Patched by core rule	Y
CVE-2026-26889	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_category.php.	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_category.php.	Patched by core rule	Y
CVE-2026-26888	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_stock.php.	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_stock.php.	Patched by core rule	Y
CVE-2026-26887	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_supplier.php.	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_supplier.php.	Patched by core rule	Y
CVE-2026-26890	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_product.php.	Sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_product.php.	Patched by core rule	Y
CVE-2026-26886	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /admin/services/manage_servic	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/admin/services/manage_ser...	e.php.		
CVE-2026-26885	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /classes/Master.php?f=dele...	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /classes/Master.php?f=delete_service.	Patched by core rule	Y
CVE-2026-26884	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /msms/admin/appointments/v...	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /msms/admin/appointments/view_appointment.php.	Patched by core rule	Y
CVE-2026-26883	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /msms/classes/Master.php?f...	Sourcecodester Online Men's Salon Management System v1.0 is vulnerable to SQL Injection in /msms/classes/Master.php?f=delete_appointment.	Patched by core rule	Y
CVE-2025-70821	renren-secuity before v5.5.0 is vulnerable to SQL Injection in the BaseServiceImpl.java component	renren-secuity before v5.5.0 is vulnerable to SQL Injection in the BaseServiceImpl.java component	Patched by core rule	Y
CVE-2026-1487	The LatePoint — Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to SQL Injecti...	Vulnerability via the JSON Import due to insufficient input sanitization or output escaping. Affects versions up to and including 5.2.7.	Patched by core rule	Y
CVE-2026-26713	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/routers/cancel-order.php.	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/routers/cancel-order.php.	Patched by core rule	Y
CVE-2026-26712	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/view-ticket-admin.php.	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/view-ticket-admin.php.	Patched by core rule	Y
CVE-2026-26711	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/view-ticket.php.	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/view-ticket.php.	Patched by core rule	Y
CVE-2026-26710	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/routers/edit-orders.php.	code-projects Simple Food Order System v1.0 is vulnerable to SQL Injection in /food/routers/edit-orders.php.	Patched by core rule	Y
CVE-2026-26709	code-projects Simple Gym Management System v1.0 is vulnerable to SQL Injection in /gym/trainer_search.php.	code-projects Simple Gym Management System v1.0 is vulnerable to SQL Injection in /gym/trainer_search.php.	Patched by core rule	Y
CVE-2026-3180	The Contest Gallery — Upload & Vote Photos, Media, Sell with PayPal & Stripe plugin for WordPress is vulnerable to bl...	Vulnerability via the 'cgLostPasswordEmail' and the 'cgl_mail' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 28.1.4.	Patched by core rule	Y
CVE-2026-26707	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_supplier.php.	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_supplier.php.	Patched by core rule	Y
CVE-2026-26706	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	in /pharmacy/view_receipt.php.	/pharmacy/view_receipt.php.		
CVE-2026-26705	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_product.php.	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_product.php.	Patched by core rule	Y
CVE-2026-26704	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_category.php.	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/view_category.php.	Patched by core rule	Y
CVE-2026-26708	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_user.php.	sourcecodester Pharmacy Point of Sale System v1.0 is vulnerable to SQL Injection in /pharmacy/manage_user.php.	Patched by core rule	Y
CVE-2026-26700	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/edit_employee.php.	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/edit_employee.php.	Patched by core rule	Y
CVE-2026-26701	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/edit_tecnical_u...	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/edit_tecnical_user.php.	Patched by core rule	Y
CVE-2026-26703	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/advance_search....	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/advance_search.php.	Patched by core rule	Y
CVE-2026-26702	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/myitem_reuse.php.	sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/myitem_reuse.php.	Patched by core rule	Y
CVE-2026-26696	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordteacher_edit.php.	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordteacher_edit.php.	Patched by core rule	Y
CVE-2026-26695	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordstudent_edit.php.	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordstudent_edit.php.	Patched by core rule	Y
CVE-2026-26694	code-projects Simple Student Alumni System v1.0 is vulnerale to SQL Injection in /TracerStudy/modal_view.php.	code-projects Simple Student Alumni System v1.0 is vulnerale to SQL Injection in /TracerStudy/modal_view.php.	Patched by core rule	Y
CVE-2025-50192	Chamilo is a learning management system.	Prior to version 1.11.30, there is a time-based SQL Injection in found in /main/webservices/registration.soap.php. This issue has been patched in version 1.11.30.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-50191	Chamilo is a learning management system.	Prior to version 1.11.30, there is an error-based SQL Injection via POST userFile with the /main/exercise/hotpotatoes.php script. This issue has been patched in version 1.11.30.	Patched by core rule	Y
CVE-2025-50190	Chamilo is a learning management system.	Prior to version 1.11.30, there is an error-based SQL Injection via the GET openid.assoc_handle parameter with the /index.php script. This issue has been patched in version 1.11.30.	Patched by core rule	Y
CVE-2025-50189	Chamilo is a learning management system.	Prior to version 1.11.30, the application performs insufficient validation of data coming from the user from the POST resource[document][SQL_INJECTION_HERE] and POST login parameters found in /main/coursecopy/copy_course_session_selected.php, which allows an attacker to perform an attack aimed at modifying the database query logic by injecting an arbitrary SQL statements. This issue has been patched in version 1.11.30.	Patched by core rule	Y
CVE-2025-50188	Chamilo is a learning management system.	Prior to version 1.11.30, the application performs insufficient validation of data coming from the user from the GET value parameter with the following scripts: /plugin/vchamilo/views/syncparams.php and /plugin/vchamilo/ajax/service.php, which allows an attacker to perform an attack aimed at modifying the database query logic by injecting an arbitrary SQL statements. This issue has been patched in version 1.11.30.	Patched by core rule	Y
CVE-2026-26698	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/modal_edit.php.	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/modal_edit.php.	Patched by core rule	Y
CVE-2026-26697	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordteacher_view.php...	code-projects Simple Student Alumni System v1.0 is vulnerable to SQL Injection in /TracerStudy/recordteacher_view.php?teacherID=.	Patched by core rule	Y
CVE-2026-3413	itsourcecode University Management System — SQL Injection via id	This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-3411	itsourcecode University Management System — SQL Injection	The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-3410	itsourcecode Society Management System — SQL Injection	Executing a manipulation of the argument student_id can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		public and could be used for attacks.		
CVE-2026-3406	projectworlds Online Art Gallery Shop — SQL Injection via fname	The impacted element is an unknown function of the file /admin/registration.php of the component Registration Handler. The manipulation of the argument fname results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-28562	wpForo 2.4.14 contains an unauthenticated SQL injection vulnerability in Topics::get_topics() where the ORDER BY clau...	Attackers exploit the wpfob parameter with CASE WHEN payloads to perform blind boolean extraction of credentials from the WordPress database.	Patched by core rule	Y
CVE-2025-13673	The Tutor LMS — eLearning and online course solution plugin for WordPress is vulnerable to SQL Injection via the 'cou...	Vulnerability via the 'coupon_code' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 3.9.6.	Patched by core rule	Y
CVE-2026-28516	openDCIM version 23.04, through commit 4467e9c4, contains a SQL injection vulnerability in Config::UpdateParameter.	The install.php and container-install.php handlers pass user-supplied input directly into SQL statements using string interpolation without prepared statements or proper input sanitation. An authenticated user can execute arbitrary SQL statements against the underlying database.	Patched by core rule	Y
CVE-2019-25497	osCommerce 2.3.4.1 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send GET requests to shopping_cart.php with malicious currency values using boolean-based SQL injection payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25496	osCommerce 2.3.4.1 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can modify the products_id value in product_info.php requests and append boolean-based SQL injection payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25495	osCommerce 2.3.4.1 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate databas...	Attackers can send GET requests to product_reviews_write.php with malicious reviews_id values using boolean-based SQL injection payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25494	Homey BNB V4 contains an SQL injection vulnerability in the administration panel login that allows unauthenticated at...	Attackers can submit SQL operators like '=' 'or' in both credentials to manipulate the authentication query and gain unauthorized access to the admin panel.	Patched by core rule	Y
CVE-2019-25493	Homey BNB V4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database que...	Attackers can send GET requests to the admin/getrecord.php endpoint with malicious 'val' values to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25492	Homey BNB V4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database que...	Attackers can send GET requests to the admin/getcmsdata.php endpoint with malicious 'pt' values to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25491	Homey BNB V4 contains an	Attackers can send GET requests	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	SQL injection vulnerability that allows unauthenticated attackers to manipulate database que...	to the admin/cms_getpagetitle.php endpoint with malicious catid values to extract sensitive database information.	rule	
CVE-2019-25490	Homey BNB V4 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database quer...	Attackers can send GET requests to the admin/edit.php endpoint with time-based SQL injection payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25489	Homey BNB V4 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database quer...	Attackers can send GET requests to the rooms/ajax_refresh_subtotal endpoint with malicious hosting_id values to extract sensitive database information or cause denial of service.	Patched by core rule	Y
CVE-2026-2831	The MailArchiver plugin for WordPress is vulnerable to SQL Injection via the 'logid' parameter in all versions up to,...	Vulnerability via the 'logid' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 4.5.0.	Patched by core rule	Y
CVE-2026-3292	jizhiCMS up to — SQL Injection	The manipulation of the argument data leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3287	youlaitech youlai-mall — SQL Injection	Performing a manipulation of the argument sortField/sort results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-28226	Phishing Club is a phishing simulation and man-in-the-middle framework.	Prior to version 1.30.2, an authenticated SQL injection vulnerability exists in the GetOrphaned recipient listing endpoint in versions prior to v1.30.2. The endpoint constructs a raw SQL query and concatenates the user-controlled sortBy value directly into the ORDER BY clause without allowlist validation. Because unknown values are silently passed through `RemapOrderBy()`, an authenticated attacker can inject SQL expressions into the `ORDER BY` clause. This issue was patched in v1.30.	Patched by core rule	Y
CVE-2026-3261	itsourcecode School Management System — SQL Injection via id	This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-28136	WP SMS — SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VeronaLabs WP SMS wp-sms allows SQL Injection.This issue affects WP	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		SMS: from n/a through <= 6.9.12.		
CVE-2026-25746	OpenEMR is a free and open source electronic health records and medical practice management application.	Versions prior to 8.0.0 contain a SQL injection vulnerability in prescription that can be exploited by authenticated attackers. The vulnerability exists due to insufficient input validation in the prescription listing functionality. Version 8.0.0 fixes the vulnerability.	Patched by core rule	Y
CVE-2026-24908	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to version 8.0.0, an SQL injection vulnerability in the Patient REST API endpoint allows authenticated users with API access to execute arbitrary SQL queries through the `_sort` parameter. This could potentially lead to database access, PHI (Protected Health Information) exposure, and credential compromise. The issue occurs when user-supplied sort field names are used in ORDER BY clauses without proper validation or identifier escaping. Version 8.0.0 fixes the issue.	Patched by core rule	Y
CVE-2026-23627	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to version 8.0.0, an SQL injection vulnerability in the Immunization module allows any authenticated user to execute arbitrary SQL queries, leading to complete database compromise, PHI exfiltration, credential theft, and potential remote code execution. The vulnerability exists because user-supplied `patient_id` values are directly concatenated into SQL WHERE clauses without parameterization or escaping. Version 8.0.0 patches the issue.	Patched by core rule	Y

Server-Side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33407	Wallos is an open-source, self-hostable personal subscription tracker.	Prior to version 4.7.0, Wallos endpoints/logos/search.php accepts HTTP_PROXY and HTTPS_PROXY environment variables without validation, enabling SSRF via proxy hijacking. The server performs DNS resolution on user-supplied search terms, which can be controlled by attackers to trigger outbound requests to arbitrary domains. This issue has been patched in version 4.7.0.	Patched by core rule	Y
CVE-2026-33401	Wallos is an open-source, self-hostable personal subscription tracker.	Prior to version 4.7.0, the patch introduced in commit e8a513591 (CVE-2026-30840) added SSRF protection to notification test endpoints but left three additional attack surfaces unprotected: the AI Ollama host parameter, the AI recommendations endpoint, and the notification cron job. An authenticated user can reach internal network services, cloud metadata endpoints (AWS IMDSv1, GCP, Azure IMDS), or localhost-bound services by supplying a crafted URL to any of these endpoints.	Patched by core rule	Y
CVE-2026-33399	Wallos is an open-source, self-hostable personal subscription tracker.	Prior to version 4.7.0, the SSRF fix applied in version 4.6.2 for CVE-2026-30839 and CVE-2026-30840 is incomplete. The validate_webhook_url_for_ssrf() protection was added to the test* notification endpoints but not to the corresponding save* endpoints. An authenticated user can save an internal/private IP address as a notification URL, and when the cron job sendnotifications.php executes, the request is sent to the internal IP without any SSRF validation.	Patched by core rule	Y
CVE-2026-33675	Vikunja is an open-source self-hosted task management platform.	Prior to version 2.2.1, the migration helper functions `DownloadFile` and `DownloadFileWithHeaders` in `pkg/modules/migration/helpers.go` make arbitrary HTTP GET requests without any SSRF protection. When a user triggers a Todoist or Trello migration, file attachment URLs from the third-party API response are passed directly to these functions, allowing an attacker to force the Vikunja server to fetch internal network resources and return the response as a downloadable task attachment.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33502	WWBN AVideo is an open source video platform.	Commit 1e6cf03e93b5a5318204b010ea28440b0d9a5ab3 contains a patch.	Patched by core rule	Y
CVE-2026-33480	WWBN AVideo is an open source video platform.	Commit 75ce8a579a58c9d4c7aafe453fbced002cb8f373 contains a patch.	Patched by core rule	Y
CVE-2026-33351	WWBN AVideo is an open source video platform.	No authentication, origin validation, or URL allowlisting is performed. Version 26.0 contains a patch for the issue.	Patched by core rule	Y
CVE-2026-33294	WWBN AVideo is an open source video platform.	An authenticated attacker can force the server to make HTTP requests to internal network resources and retrieve the responses by viewing the saved video thumbnail. Version 26.0 fixes the issue.	Patched by core rule	Y
CVE-2026-4528	A vulnerability was determined in trueleaf ApiFlow 0.9.7.	The impacted element is the function validateUrlSecurity of the file packages/server/src/service/proxy/http_proxy.service.ts of the component URL Validation Handler. This manipulation causes server-side request forgery. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-33237	WWBN AVideo is an open source video platform.	Unlike other AVideo endpoints that were recently patched for SSRF (GHSA-9x67-f2v7-63rw, GHSA-h39h-7cvg-q7j6), the Scheduler's callback URL is never passed through `isSSRFSafeURL()`, which blocks requests to RFC-1918 private addresses, loopback, and cloud metadata endpoints. An admin can configure a scheduled task with an internal network `callbackURL` to perform SSRF against cloud infrastructure metadata services or internal APIs not otherwise reachable from the internet. Version 26.	Patched by core rule	Y
CVE-2026-33226	Budibase is a low code platform for creating internal tools, workflows, and admin panels.	In versions from 3.30.6 and prior, the REST datasource query preview endpoint (POST /api/queries/preview) makes server-side HTTP requests to any URL supplied by the user in fields.path with no validation. An authenticated admin can reach internal services that are not exposed to the internet — including cloud metadata endpoints (AWS/GCP/Azure), internal databases, Kubernetes APIs, and other pods on the internal network.	Patched by core rule	Y
CVE-2026-33126	Frigate is a network video recorder (NVR) with realtime local object detection for IP cameras.	Prior to version 0.16.3, the /ffprobe endpoint accepts arbitrary user-controlled URLs without proper	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		validation, allowing Server-Side Request Forgery (SSRF) attacks. An attacker can use the Frigate server to make HTTP requests to internal network resources, cloud metadata services, or perform port scanning. This issue has been patched in version 0.16.3.		
CVE-2026-33081	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser.	Versions 0.8.2 and below have a Blind SSRF vulnerability in the /download endpoint. The validateDownloadURL() function only checks the initial user-supplied URL, but the embedded Chromium browser can follow attacker-controlled redirects/navigations to internal network addresses after validation. Exploitation requires security.allowDownload=true (disabled by default), limiting real-world impact.	Patched by core rule	Y
CVE-2026-33039	WWBN AVideo is an open source video platform.	In versions 25.0 and below, the plugin/LiveLinks/proxy.php endpoint validates user-supplied URLs against internal/private networks using isSSRFSafeURL(), but only checks the initial URL. When the initial URL responds with an HTTP redirect (Location header), the redirect target is fetched via fakeBrowser() without re-validation, allowing an attacker to reach internal services (cloud metadata, RFC1918 addresses) through an attacker-controlled redirect. This issue is fixed in version 26.0.	Patched by core rule	Y
CVE-2026-32949	SQLBot is an intelligent data query system based on a large language model and RAG.	Versions prior to 1.7.0 contain a Server-Side Request Forgery (SSRF) vulnerability that allows an attacker to retrieve arbitrary system and application files from the server. An attacker can exploit the /api/v1/datasource/check endpoint by configuring a forged MySQL data source with a malicious parameter extraJdbc="local_infile=1".	Patched by core rule	Y
CVE-2026-32812	Admidio is an open-source user management solution.	In versions 5.0.0 through 5.0.6, unrestricted URL fetch in the SSO Metadata API can result in SSRF and local file reads. The SSO Metadata fetch endpoint at modules/sso/fetch_metadata.php accepts an arbitrary URL via $_GET['url'], validates it only with PHP's FILTER_VALIDATE_URL, and passes it directly to file_get_contents(). FILTER_VALIDATE_URL accepts file://, http://, ftp://, data://, and php:// scheme URIs.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33321	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.2, users with the `Notes - my encounters` role can fill Eye Exam forms in patient encounters. The answers to the form can be printed out in PDF form. An Out-of-Band Server-Side Request Forgery (OOB SSRF) vulnerability was identified in the PDF creation function where the form answers are parsed as unescaped HTML, allowing an attacker to forge requests from the server made to external or internal resources. Version 8.0.0.2 fixes the issue.	Patched by core rule	Y
CVE-2026-3632	A flaw was found in libsoup, a library used by applications to send network requests.	This vulnerability occurs because libsoup does not properly validate hostnames, allowing special characters to be injected into HTTP headers. A remote attacker could exploit this to perform HTTP smuggling, where they can send hidden, malicious requests alongside legitimate ones. In certain situations, this could lead to Server-Side Request Forgery (SSRF), enabling an attacker to force the server to make unauthorized requests to other internal or external systems.	Patched by core rule	Y
CVE-2026-4308	A weakness has been identified in frdel/agent0ai agent-zero 0.9.7.	This manipulation causes server-side request forgery. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-32301	Centrifugo is an open-source scalable real-time messaging server.	Prior to 6.7.0, Centrifugo is vulnerable to Server-Side Request Forgery (SSRF) when configured with a dynamic JWKS endpoint URL using template variables (e.g. {{tenant}}). An unauthenticated attacker can craft a JWT with a malicious iss or aud claim value that gets interpolated into the JWKS fetch URL before the token signature is verified, causing Centrifugo to make an outbound HTTP request to an attacker-controlled destination. This vulnerability is fixed in 6.7.0.	Patched by core rule	Y
CVE-2026-32133	2FAuth is a web app to manage Two-Factor Authentication (2FA) accounts and generate their security codes.	Prior to 6.1.0, a blind SSRF vulnerability exists in 2FAuth that allows authenticated users to make arbitrary HTTP requests from the server to internal networks and cloud metadata endpoints. The image parameter in OTP URL is not properly validated for internal / private IP addresses before making HTTP requests. While the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		previous fix added response validation to ensure only valid images are stored but HTTP request is still made to arbitrary URLs before this validation occurs.		
CVE-2026-32110	SiYuan is a personal knowledge management system.	Prior to 3.6.0, the /api/network/forwardProxy endpoint allows authenticated users to make arbitrary HTTP requests from the server. The endpoint accepts a user-controlled URL and makes HTTP requests to it, returning the full response body and headers. There is no URL validation to prevent requests to internal networks, localhost, or cloud metadata services. This vulnerability is fixed in 3.6.0.	Patched by core rule	Y
CVE-2026-31829	Flowise is a drag & drop user interface to build a customized large language model flow.	Prior to 3.0.13, Flowise exposes an HTTP Node in AgentFlow and Chatflow that performs server-side HTTP requests using user-controlled URLs. By default, there are no restrictions on target hosts, including private/internal IP ranges (RFC 1918), localhost, or cloud metadata endpoints.	Patched by core rule	Y
CVE-2026-25960	vLLM is an inference and serving engine for large language models (LLMs).	The SSRF protection fix for CVE-2026-24779 add in 0.15.1 can be bypassed in the load_from_url_async method due to inconsistent URL parsing behavior between the validation layer and the actual HTTP client. The SSRF fix uses urllib3.util.parse_url() to validate and extract the hostname from user-provided URLs. However, load_from_url_async uses aiohttp for making the actual HTTP requests, and aiohttp internally uses the yarl library for URL parsing. This vulnerability in 0.17.0.	Patched by core rule	Y
CVE-2026-3789	A vulnerability was detected in Bytedesk up to 1.3.9.	Affected is the function getModels of the file source-code/src/main/java/com/bytedesk/ai/springai/providers/gitee/SpringAIGiteeRestService.java of the component SpringAIGiteeRestController. Performing a manipulation of the argument apiUrl results in server-side request forgery. Remote exploitation of the attack is possible. The exploit is now public and may be used. Upgrading to version 1.4.5.4 is able to address this issue. The patch is named 975e39e4dd527596987559f56c5f9f973f64eff7.	Patched by core rule	Y
CVE-2026-3788	A security vulnerability has been detected in Bytedesk up to 1.3.9.	Such manipulation of the argument apiUrl leads to server-side request forgery. The attack may be launched remotely. The exploit has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been disclosed publicly and may be used. Upgrading to version 1.4.5.4 will fix this issue. The name of the patch is 975e39e4dd527596987559f56c5f9f973f64eff7. It is recommended to upgrade the affected component.		
CVE-2026-3750	A security vulnerability has been detected in ContiNew Admin up to 4.2.0.	The manipulation leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-30858	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval.	Prior to version 0.3.0, a DNS rebinding vulnerability in the web_fetch tool allows an unauthenticated attacker to bypass URL validation and access internal resources on the server, including private IP addresses (e.g., 127.0.0.1, 192.168.x.x). By crafting a malicious domain that resolves to a public IP during validation and subsequently resolves to a private IP during execution, an attacker can access sensitive local services and potentially exfiltrate data.	Patched by core rule	Y
CVE-2026-30834	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser.	Prior to version 0.7.7, a Server-Side Request Forgery (SSRF) vulnerability in the /download endpoint allows any user with API access to induce the PinchTab server to make requests to arbitrary URLs, including internal network services and local system files, and exfiltrate the full response content. This issue has been patched in version 0.7.7.	Patched by core rule	Y
CVE-2026-30832	Soft Serve is a self-hostable Git server for the command line.	From version 0.6.0 to before version 0.11.4, an authenticated SSH user can force the server to make HTTP requests to internal/private IP addresses by running repo import with a crafted --lfs-endpoint URL. The initial batch request is blind (the response from a metadata endpoint won't parse as valid LFS JSON), but an attacker hosting a fake LFS server can chain this into full read access to internal services by returning download URLs that point at internal targets.	Patched by core rule	Y
CVE-2026-30839	Wallos is an open-source, self-hostable personal subscription tracker.	Prior to version 4.6.2, testwebhooknotifications.php does not validate the target URL against private/reserved IP ranges, enabling full-read SSRF. The server response is returned to the caller. This issue has been patched in version 4.6.2.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-27797	Homarr is an open-source dashboard.	Prior to version 1.54.0, an unauthenticated Server-Side Request Forgery (SSRF) vulnerability allows a remote attacker to force the Homarr server to perform arbitrary outbound HTTP requests. This can be used as an internal network access primitive (e.g., reaching loopback/private ranges) from the Homarr host/container network context. This issue has been patched in version 1.54.0.	Patched by core rule	Y
CVE-2026-30247	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval.	Prior to version 0.2.12, the application's "Import document via URL" feature is vulnerable to Server-Side Request Forgery (SSRF) through HTTP redirects. While the backend implements comprehensive URL validation (blocking private IPs, loopback addresses, reserved hostnames, and cloud metadata endpoints), it fails to validate redirect targets. An attacker can bypass all protections by using a redirect chain, forcing the server to access internal services.	Patched by core rule	Y
CVE-2026-28508	Idno is a social publishing platform.	Prior to version 1.6.4, a logic error in the API authentication flow causes the CSRF protection on the URL unfurl service endpoint to be trivially bypassed by any unauthenticated remote attacker. Combined with the absence of a login requirement on the endpoint itself, this allows an attacker to force the server to make arbitrary outbound HTTP requests to any host, including internal network addresses and cloud instance metadata services, and retrieve the response content.	Patched by core rule	Y
CVE-2026-28467	OpenClaw versions prior to 2026.2.2 contain a server-side request forgery vulnerability in attachment and media URL h...	OpenClaw versions prior to 2026.2.2 contain a server-side request forgery vulnerability in attachment and media URL hydration that allows remote attackers to fetch arbitrary HTTP(S) URLs. Attackers who can influence media URLs through model-controlled sendAttachment or auto-reply mechanisms can trigger SSRF to internal resources and exfiltrate fetched response bytes as outbound attachments.	Patched by core rule	Y
CVE-2025-50199	Chamilo is a learning management system.	Prior to version 1.11.30, there is a blind SSRF vulnerability in /index.php via the POST openid_url parameter. This issue has been patched in version 1.11.30.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-50337	Chamilo is a learning management system.	Prior to version 1.11.28, the OpenId function allows anyone to send requests to any URL on server's behalf, which results in unauthenticated blind SSRF. This issue has been patched in version 1.11.28.	Patched by core rule	Y
CVE-2026-3286	A vulnerability was identified in itwanger paicoding 1.0.0/1.0.1/1.0.2/1.0.3.	The impacted element is the function Save of the file paicoding-web/src/main/java/com/github/paicoding/forum/web/common/image/rest/ImageRestController.java of the component Image Save Endpoint. Such manipulation of the argument img leads to server-side request forgery. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3270	A vulnerability has been found in psi-probe PSI Probe up to 5.3.0.	The manipulation leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-27829	Astro is a web framework.	In versions 9.0.0 through 9.5.3, a bug in Astro's image pipeline allows bypassing `image.domains` / `image.remotePatterns` restrictions, enabling the server to fetch content from unauthorized remote hosts. Astro provides an `inferSize` option that fetches remote images at render time to determine their dimensions. Remote image fetches are intended to be restricted to domains the site developer has manually authorized (using the `image.domains` or `image.remotePatterns` options).	Patched by core rule	Y
CVE-2026-27808	Mailpit is an email testing tool and API for developers.	Prior to version 1.29.2, the Link Check API (/api/v1/message/{ID}/link-check) is vulnerable to Server-Side Request Forgery (SSRF). The server performs HTTP HEAD requests to every URL found in an email without validating target hosts or filtering private/internal IP addresses. The response returns status codes and status text per link, making this a non-blind SSRF. In the default configuration (no authentication on SMTP or API), this is fully exploitable remotely with zero user interaction.	Patched by core rule	Y
CVE-2026-24005	Kruise provides automated management	Kruise provides automated management of large-scale	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	of large-scale applications on Kubernetes.	applications on Kubernetes. Prior to versions 1.8.3 and 1.7.5, PodProbeMarker allows defining custom probes with TCPSocket or HTTPGet handlers. The webhook validation does not restrict the Host field in these probe configurations. Since kruise-daemon runs with hostNetwork=true, it executes probes from the node network namespace.		
CVE-2026-33407	Wallos is an open-source, self-hostable personal subscription tracker.	Prior to version 4.7.0, Wallos endpoints/logos/search.php accepts HTTP_PROXY and HTTPS_PROXY environment variables without validation, enabling SSRF via proxy hijacking. The server performs DNS resolution on user-supplied search terms, which can be controlled by attackers to trigger outbound requests to arbitrary domains. This issue has been patched in version 4.7.0.	Patched by core rule	Y

Cross Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-32545	Taboola Pixel — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Taboola Taboola Pixel taboola-pixel allows Reflected XSS.This issue affects Taboola Pixel: from n/a through <= 1.1.4.	Patched by core rule	Y
CVE-2026-32544	OOPSpam Anti-Spam — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OOPSpam Team OOPSpam Anti-Spam oopspam-anti-spam allows Stored XSS.This issue affects OOPSpam Anti-Spam: from n/a through <= 1.2.62.	Patched by core rule	Y
CVE-2026-32542	Fusion Builder — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeFusion Fusion Builder fusion-builder allows Reflected XSS.This issue affects Fusion Builder: from n/a through < 3.15.0.	Patched by core rule	Y
CVE-2026-32540	Bookly — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bookly Bookly bookly-responsive-appointment-booking-tool allows Reflected XSS.This issue affects Bookly: from n/a through <= 26.7.	Patched by core rule	Y
CVE-2026-32532	Contact Form & Lead Form Elementor Builder — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeHunk Contact Form & Lead Form Elementor Builder lead-form-builder allows Stored XSS.This issue affects Contact Form & Lead Form Elementor Builder: from n/a through <= 2.0.1.	Patched by core rule	Y
CVE-2026-32529	Molla — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in don-themes Molla molla allows Reflected XSS.This issue affects Molla: from n/a through < 1.5.19.	Patched by core rule	Y
CVE-2026-32528	Riode — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in don-themes Riode riode allows Reflected XSS.This issue affects Riode: from n/a through < 1.6.29.	Patched by core rule	Y
CVE-2026-32526	Abandoned Cart Recovery for WooCommerce — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme Abandoned Cart Recovery for WooCommerce woo-abandoned-cart-recovery allows Stored XSS.This issue affects Abandoned Cart Recovery for WooCommerce: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through <= 1.1.10.		
CVE-2026-32521	WP Custom Admin Interface — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Northern Beaches Websites WP Custom Admin Interface wp-custom-admin-interface allows DOM-Based XSS.This issue affects WP Custom Admin Interface: from n/a through <= 7.42.	Patched by core rule	Y
CVE-2026-32518	Gaea — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in imithemes Gaea gaea allows Reflected XSS.This issue affects Gaea: from n/a through < 3.8.	Patched by core rule	Y
CVE-2026-32517	Contact Manager — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kleor Contact Manager contact-manager allows Reflected XSS.This issue affects Contact Manager: from n/a through <= 9.1.	Patched by core rule	Y
CVE-2026-32494	Image Slider by Ays — Exploiting Incorrectly Configured Access Control Security Levels	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro Image Slider by Ays ays-slider allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Image Slider by Ays: from n/a through <= 2.7.1.	Patched by core rule	Y
CVE-2026-32493	JobSearch — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eyecix JobSearch wp-jobsearch allows Reflected XSS.This issue affects JobSearch: from n/a through <= 3.2.0.	Patched by core rule	Y
CVE-2026-32491	WP Review Slider — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jgwhite33 WP Review Slider wp-facebook-reviews allows Stored XSS.This issue affects WP Review Slider: from n/a through <= 13.9.	Patched by core rule	Y
CVE-2026-32490	WP TripAdvisor Review Slider — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jgwhite33 WP TripAdvisor Review Slider wp-tripadvisor-review-slider allows Stored XSS.This issue affects WP TripAdvisor Review Slider: from n/a through <= 14.1.	Patched by core rule	Y
CVE-2026-31914	WP Courses LMS — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hookandhook WP Courses LMS wp-courses allows DOM-Based XSS.This issue affects WP Courses LMS: from n/a through <= 3.2.26.	Patched by core rule	Y
CVE-2026-27088	Darna Framework — Reflected XSS	Improper Neutralization of Input During Web Page Generation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		('Cross-site Scripting') vulnerability in G5Theme Darna Framework darna-framework allows Reflected XSS.This issue affects Darna Framework: from n/a through <= 2.9.		
CVE-2026-27087	Wolverine Framework — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in G5Theme Wolverine Framework wolverine-framework allows Reflected XSS.This issue affects Wolverine Framework: from n/a through <= 1.9.	Patched by core rule	Y
CVE-2026-27054	Penci Soledad Data Migrator — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Soledad Data Migrator penci-data-migrator allows Reflected XSS.This issue affects Penci Soledad Data Migrator: from n/a through <= 1.3.1.	Patched by core rule	Y
CVE-2026-25465	CP Multi View Event Calendar — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codepeople CP Multi View Event Calendar cp-multi-view-calendar allows Stored XSS.This issue affects CP Multi View Event Calendar : from n/a through <= 1.4.35.	Patched by core rule	Y
CVE-2026-25461	Listeo Core — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in purethemes Listeo Core listeo-core allows Reflected XSS.This issue affects Listeo Core: from n/a through <= 2.0.21.	Patched by core rule	Y
CVE-2026-25452	Remoji — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDO Remoji remoji allows Stored XSS.This issue affects Remoji: from n/a through <= 2.2.	Patched by core rule	Y
CVE-2026-25435	Booking calendar, Appointment Booking System — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpdevart Booking calendar, Appointment Booking System booking-calendar allows Stored XSS.This issue affects Booking calendar, Appointment Booking System: from n/a through <= 3.2.36.	Patched by core rule	Y
CVE-2026-25417	ProfileGrid — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss ProfileGrid profilegrid-user-profiles-groups-and-communities allows Stored XSS.This issue affects ProfileGrid : from n/a through <= 5.9.8.1.	Patched by core rule	Y
CVE-2026-25383	KiviCare — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Iqonic Design	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		KiviCare kivicare-clinic-management-system allows Reflected XSS.This issue affects KiviCare: from n/a through <= 3.6.16.		
CVE-2026-25376	Addon Jobsearch Chat — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eyecix Addon Jobsearch Chat addon-jobsearch-chat allows Reflected XSS.This issue affects Addon Jobsearch Chat: from n/a through <= 3.0.	Patched by core rule	Y
CVE-2026-25373	Vayvo — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ProgressionStudios Vayvo vayvo-progression allows Reflected XSS.This issue affects Vayvo: from n/a through < 6.8.	Patched by core rule	Y
CVE-2026-25361	WpEvently — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in magepeopleteam WpEvently mage-eventpress allows Reflected XSS.This issue affects WpEvently: from n/a through <= 5.1.4.	Patched by core rule	Y
CVE-2026-25356	Yobazar — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Yobazar yobazar allows Reflected XSS.This issue affects Yobazar: from n/a through < 1.6.7.	Patched by core rule	Y
CVE-2026-25355	Sanzo — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Sanzo sanzo allows Stored XSS.This issue affects Sanzo: from n/a through < 2.4.3.	Patched by core rule	Y
CVE-2026-25354	Reebox — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Reebox reebox allows Reflected XSS.This issue affects Reebox: from n/a through < 1.4.8.	Patched by core rule	Y
CVE-2026-25353	Nooni — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Nooni nooni allows Reflected XSS.This issue affects Nooni: from n/a through < 1.5.1.	Patched by core rule	Y
CVE-2026-25352	MyDecor — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup MyDecor mydecor allows Reflected XSS.This issue affects MyDecor: from n/a through < 1.5.9.	Patched by core rule	Y
CVE-2026-25351	MyMedi — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability in skygroup MyMedi mymedi allows Reflected XSS.This issue affects MyMedi: from n/a through < 1.7.7.		
CVE-2026-25350	Miti — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Miti miti allows Reflected XSS.This issue affects Miti: from n/a through < 1.5.3.	Patched by core rule	Y
CVE-2026-25349	Loobek — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Loobek loobek allows Reflected XSS.This issue affects Loobek: from n/a through < 1.5.2.	Patched by core rule	Y
CVE-2026-25347	WP REST Cache — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Acato WP REST Cache wp-rest-cache allows Stored XSS.This issue affects WP REST Cache: from n/a through <= 2026.1.0.	Patched by core rule	Y
CVE-2026-25346	FAQ Builder AYS — Exploiting Incorrectly Configured Access Control Security Levels	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ays Pro FAQ Builder AYS faq-builder-ays allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FAQ Builder AYS: from n/a through <= 1.8.2.	Patched by core rule	Y
CVE-2026-25342	Boutique — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kutethemes Boutique kute-boutique allows Reflected XSS.This issue affects Boutique: from n/a through < 2.4.6.	Patched by core rule	Y
CVE-2026-25341	RSFirewall! — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RSJoomla! RSFirewall! rsfirewall allows Stored XSS.This issue affects RSFirewall!: from n/a through <= 1.1.45.	Patched by core rule	Y
CVE-2026-25306	XStore Core — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme XStore Core et-core-plugin allows Reflected XSS.This issue affects XStore Core: from n/a through <= 5.6.4.	Patched by core rule	Y
CVE-2026-25304	Jaroti — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Jaroti jaroti allows Reflected XSS.This issue affects Jaroti: from n/a through < 1.4.8.	Patched by core rule	Y
CVE-2026-25033	Motta Addons — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability in uixthemes Motta Addons motta-addons allows Reflected XSS.This issue affects Motta Addons: from n/a through < 1.6.1.		
CVE-2026-25025	VikRestaurants — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikRestaurants vikrestaurants allows Reflected XSS.This issue affects VikRestaurants: from n/a through <= 1.5.2.	Patched by core rule	Y
CVE-2026-25018	NaturaLife Extensions — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in stmcan NaturaLife Extensions naturalife-extensions allows Reflected XSS.This issue affects NaturaLife Extensions: from n/a through <= 2.1.	Patched by core rule	Y
CVE-2026-25013	Phox Hosting — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WHMCSdes Phox Hosting phox-host allows Reflected XSS.This issue affects Phox Hosting: from n/a through <= 2.0.8.	Patched by core rule	Y
CVE-2026-24983	UpSolution Core — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UpSolution UpSolution Core us-core allows Reflected XSS.This issue affects UpSolution Core: from n/a through <= 8.41.	Patched by core rule	Y
CVE-2026-24980	Visionary Core — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Visionary Core noo-visionary-core allows Reflected XSS.This issue affects Visionary Core: from n/a through <= 1.4.9.	Patched by core rule	Y
CVE-2026-24979	Jobica Core — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobica Core jobica-core allows Reflected XSS.This issue affects Jobica Core: from n/a through <= 1.4.1.	Patched by core rule	Y
CVE-2026-24975	Organici Library — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Organici Library noo-organici-library allows Reflected XSS.This issue affects Organici Library: from n/a through <= 2.1.2.	Patched by core rule	Y
CVE-2026-24973	CitiLights — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme CitiLights noo-citilights allows Reflected XSS.This issue affects CitiLights: from n/a through <= 3.7.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-24391	Car Dealer — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeMakers Car Dealer cardealer allows Reflected XSS.This issue affects Car Dealer: from n/a through <= 1.6.7.	Patched by core rule	Y
CVE-2026-24370	The Grid — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Theme-one The Grid the-grid allows Stored XSS.This issue affects The Grid: from n/a through < 2.8.0.	Patched by core rule	Y
CVE-2026-23979	Gyan Elements — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Softwebmedia Gyan Elements gyan-elements allows Reflected XSS.This issue affects Gyan Elements: from n/a through <= 2.2.1.	Patched by core rule	Y
CVE-2026-23973	Golo — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uxper Golo golo allows Reflected XSS.This issue affects Golo: from n/a through < 1.7.5.	Patched by core rule	Y
CVE-2026-23807	WP Telegram Widget and Join Link — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Socio WP Telegram Widget and Join Link wptelegram-widget allows Reflected XSS.This issue affects WP Telegram Widget and Join Link: from n/a through <= 2.2.13.	Patched by core rule	Y
CVE-2026-22524	Legacy Admin — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themepassion Legacy Admin legacy-admin allows Reflected XSS.This issue affects Legacy Admin: from n/a through <= 9.5.	Patched by core rule	Y
CVE-2026-22523	Ultra WordPress Admin — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themepassion Ultra WordPress Admin ultra-admin allows Reflected XSS.This issue affects Ultra WordPress Admin: from n/a through <= 11.7.	Patched by core rule	Y
CVE-2026-22520	Handmade Framework — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in G5Theme Handmade Framework handmade-framework allows Reflected XSS.This issue affects Handmade Framework: from n/a through <= 3.9.	Patched by core rule	Y
CVE-2026-22491	My auctions allegro — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wphocus My auctions allegro my-auctions-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allegro-free-edition allows Reflected XSS.This issue affects My auctions allegro: from n/a through <= 3.6.35.		
CVE-2025-69096	Zorka — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in G5Theme Zorka zorka allows Reflected XSS.This issue affects Zorka: from n/a through <= 1.5.7.	Patched by core rule	Y
CVE-2026-4766	The Easy Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Gallery shortcode po...	Vulnerability via the Gallery shortcode post meta field due to insufficient input sanitization or output escaping. Affects versions up to and including 1.5.3..	Patched by core rule	Y
CVE-2026-33331	oRPC is an tool that helps build APIs that are end-to-end type-safe and adhere to OpenAPI standards.	Prior to version 1.13.9, a stored cross-site scripting (XSS) vulnerability exists in the OpenAPI documentation generation of orpc. If an attacker can control any field within the OpenAPI specification (such as info.description), they can break out of the JSON context and execute arbitrary JavaScript when a user views the generated API documentation. This issue has been patched in version 1.13.9.	Patched by core rule	Y
CVE-2026-33400	Wallos is an open-source, self-hostable personal subscription tracker.	Prior to version 4.7.0, a stored cross-site scripting (XSS) vulnerability in the payment method rename endpoint allows any authenticated user to inject arbitrary JavaScript that executes when any user visits the Settings, Subscriptions, or Statistics pages. Combined with the wallos_login authentication cookie lacking the HttpOnly flag, this enables full session hijacking. This issue has been patched in version 4.7.0.	Patched by core rule	Y
CVE-2026-30661	iCMS v8.0.0 contains a Cross-Site Scripting (XSS) vulnerability in the User Management component, specifically within...	This allows remote attackers to execute arbitrary web script or HTML via the regip or loginip parameters.	Patched by core rule	Y
CVE-2025-60948	Census CSWeb 8.0.1 allows stored cross-site scripting in user supplied fields.	Census CSWeb 8.0.1 allows stored cross-site scripting in user supplied fields. A remote, authenticated attacker could store malicious javascript that executes in a victim's browser. Fixed in 8.1.0 alpha.	Patched by core rule	Y
CVE-2026-33683	WWBN AVideo is an open source video platform.	In versions up to and including 26.0, a sanitization order-of-operations flaw in the user profile "about" field allows any registered user to inject arbitrary JavaScript that executes when other users visit their channel page. The `xss_esc()` function entity-encodes input before `strip_specific_tags()` can match dangerous HTML tags, and `html_entity_decode()` on output reverses the encoding, restoring the raw malicious	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		HTML. Commit 7cfdc380dae1e56bbb5de581470d9e9957445df0 contains a patch.		
CVE-2026-33500	WWBN AVideo is an open source video platform.	With `safeMode` disabled, Parsedown's built-in `javascript:` URI filtering (`sanitiseElement()`/`filterUnsafeUrlInAttribute()`) is also inactive. An attacker can inject stored XSS via comment markdown links. Commit 3ae02fa240939dbefc5949d64f05790fd25d728d contains a patch.	Patched by core rule	Y
CVE-2026-33499	WWBN AVideo is an open source video platform.	In versions up to and including 26.0, the `view/forbiddenPage.php` and `view/warningPage.php` templates reflect the `$_REQUEST['unlockPassword']` parameter directly into an HTML `<input>` tag's attributes without any output encoding or sanitization. An attacker can craft a URL that breaks out of the `value` attribute and injects arbitrary HTML attributes including JavaScript event handlers, achieving reflected XSS against any visitor who clicks the link.	Patched by core rule	Y
CVE-2024-51226	A stored cross-site scripting (XSS) vulnerability in the component /admin/search-vehicle.php of Phpgurukul Vehicle Re...	A stored cross-site scripting (XSS) vulnerability in the component /admin/search-vehicle.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Search parameter.	Patched by core rule	Y
CVE-2024-51225	A stored cross-site scripting (XSS) vulnerability in the component /admin/add-brand.php of Phpgurukul Vehicle Record ...	A stored cross-site scripting (XSS) vulnerability in the component /admin/add-brand.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the brandname parameter.	Patched by core rule	Y
CVE-2024-51224	Multiple cross-site scripting (XSS) vulnerabilities in the component /admin/edit-vehicle.php of Phpgurukul Vehicle Re...	Multiple cross-site scripting (XSS) vulnerabilities in the component /admin/edit-vehicle.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the vehiclename, modelnumber, regnumber, vehiclesubtype, chasisnum and enginenumber parameters.	Patched by core rule	Y
CVE-2024-51223	A stored cross-site scripting (XSS) vulnerability in the component /admin/profile.php of Phpgurukul Vehicle Record Ma...	A stored cross-site scripting (XSS) vulnerability in the component /admin/profile.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Mobile Number	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameter.		
CVE-2024-51222	A stored cross-site scripting (XSS) vulnerability in the component /admin/profile.php of Phpgurukul Vehicle Record Ma...	A stored cross-site scripting (XSS) vulnerability in the component /admin/profile.php of Phpgurukul Vehicle Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name parameter.	Patched by core rule	Y
CVE-2025-6229	The Sina Extension for Elementor (Header Builder, Footer Builter, Theme Builder, Slider, Gallery, Form, Modal, Data T...	Vulnerability via the `Fancy Text Widget` And `Countdown Widget` DOM attributes due to insufficient input sanitization or output escaping. Affects versions up to and including 3.7.0.	Patched by core rule	Y
CVE-2026-33295	WWBN AVideo is an open source video platform.	The `clean_title` field of a video record is interpolated directly into a JavaScript string literal without any escaping, allowing an attacker who can create or modify a video to inject arbitrary JavaScript that executes in the browser of any user who visits the affected download page. Version 26.0 fixes the issue.	Patched by core rule	Y
CVE-2026-3427	The Yoast SEO — Advanced SEO with real-time guidance and built-in AI plugin for WordPress is vulnerable to Stored Cro...	Vulnerability via the the `jsonText` block attribute due to insufficient input sanitization or output escaping. Affects versions up to and including 27.1.1.	Patched by core rule	Y
CVE-2026-4161	The Review Map by RevuKangaroo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin setti...	Vulnerability via the plugin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.7.	Patched by core rule	Y
CVE-2026-4086	The WP Random Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cat', 'nocat', and 't...	Vulnerability via the 'cat', 'nocat', and 'text' shortcode attributes of the 'wp_random_button' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0..	Patched by core rule	Y
CVE-2026-4084	The fyyd podcast shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fyyd-podcast',...	Vulnerability via the 'fyyd-podcast', 'fyyd-episode', and 'fyyd' shortcodes due to insufficient input sanitization or output escaping. Affects versions up to and including 0.3.1..	Patched by core rule	Y
CVE-2026-4077	The Ecover Builder For Dummies plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' paramet...	Vulnerability via the 'id' parameter of the 'ecover' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0..	Patched by core rule	Y
CVE-2026-4072	The WordPress PayPal Donation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'donate' shor...	Vulnerability via the 'donate' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.01..	Patched by core rule	Y
CVE-2026-4069	The Alfie — Feed Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'naam'	Vulnerability via the 'naam' parameter due to insufficient input sanitization or output escaping. Affects versions up to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	parameter in...	and including 1.2.1..		
CVE-2026-4067	The Ad Short plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ad' shortcode's 'client' attr...	Vulnerability via the 'ad' shortcode's 'client' attribute due to insufficient input sanitization or output escaping. Affects versions up to and including 2.0.1..	Patched by core rule	Y
CVE-2026-4022	The Show Posts list — Easy designs, filters and more plugin for WordPress is vulnerable to Stored Cross-Site Scriptin...	Vulnerability via the 'post_type' shortcode attribute in the 'swiftpost-list' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.0.	Patched by core rule	Y
CVE-2026-3997	The Text Toggle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' shortcode attribute...	Vulnerability via the 'title' shortcode attribute of the [tt_part] and [tt] shortcodes due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1..	Patched by core rule	Y
CVE-2026-3996	The WP Games Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the [game] shortcode in all ...	Vulnerability via the [game] shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 0.1.	Patched by core rule	Y
CVE-2026-3619	The Sheets2Table plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'titles' shortcode attribu...	Vulnerability via the 'titles' shortcode attribute in the [sheets2table-render-table] shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 0.4.1..	Patched by core rule	Y
CVE-2026-3617	The Paypal Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'amount' and 'name' sh...	Vulnerability via the 'amount' and 'name' shortcode attributes due to insufficient input sanitization or output escaping. Affects versions up to and including 0.3..	Patched by core rule	Y
CVE-2026-3554	The Sherk Custom Post Type Displays plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title'...	Vulnerability via the 'title' shortcode attribute due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.1..	Patched by core rule	Y
CVE-2026-3354	The Wikilookup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Popup Width' setting in all...	Vulnerability via the 'Popup Width' setting due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.5..	Patched by core rule	Y
CVE-2026-3353	The Comment SPAM Wiper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'API Key' setting in...	Vulnerability via the 'API Key' setting due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.1..	Patched by core rule	Y
CVE-2026-3347	The Multi Functional Flexi Lightbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `arv_lb...	Vulnerability via the `arv_lb[message]` parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.	Patched by core rule	Y
CVE-2026-3333	The MinhNhut Link Gateway plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'linkgat...	Vulnerability via the plugin's 'linkgate' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 3.6.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-3003	The Vagaro Booking Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'vagaro_code' par...	Vulnerability via the 'vagaro_code' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 0.3.	Patched by core rule	Y
CVE-2026-2837	The Ricerca — advanced search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin's settings...	Vulnerability via plugin's settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.12.	Patched by core rule	Y
CVE-2026-2501	The Ed's Social Share plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `social_shar...	Vulnerability via the plugin's `social_share` shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 2.0..	Patched by core rule	Y
CVE-2026-2496	The Ed's Font Awesome plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `eds_font_aw...	Vulnerability via the plugin's `eds_font_awesome` shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 2.0..	Patched by core rule	Y
CVE-2026-2440	The SurveyJS plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, ...	This is due to insufficient input sanitization and output escaping. The public survey page exposes the nonce required for submission, allowing unauthenticated attackers to submit HTML-encoded payloads that are decoded and rendered as executable HTML when an administrator views survey results, leading to stored XSS in the admin context.	Patched by core rule	Y
CVE-2026-2427	The itsukaita plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'day_from' and 'day_to' pa...	Vulnerability via the 'day_from' and 'day_to' parameters due to insufficient input sanitization or output escaping. Affects versions up to and including 0.1.2.	Patched by core rule	Y
CVE-2026-2424	The Reward Video Ad for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin setting...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.6..	Patched by core rule	Y
CVE-2026-2277	The rexCrawler plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'url' and 'regex' paramet...	Vulnerability via the 'url' and 'regex' parameters in the search-pattern tester page due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.15.	Patched by core rule	Y
CVE-2026-2121	The Weaver Show Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'add_class' parameter...	Vulnerability via the 'add_class' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.8.1..	Patched by core rule	Y
CVE-2026-1914	The FuseDesk plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's fusedesk_newcase shor...	Vulnerability via the plugin's fusedesk_newcase shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 6.8.	Patched by core rule	Y
CVE-2026-1911	The Twitter Feeds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tweet_title' parameter i...	Vulnerability via the 'tweet_title' parameter in the 'TwitterFeeds' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-1908	The Integration with Hubspot Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'hubspot...	Vulnerability via the 'hubspotform' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.2.	Patched by core rule	Y
CVE-2026-1899	The Any Post Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's aps_slider sho...	Vulnerability via the plugin's aps_slider shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.4.	Patched by core rule	Y
CVE-2026-1891	The Simple Football Scoreboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ytmr_fb_sco...	Vulnerability via the 'ytmr_fb_scoreboard' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.	Patched by core rule	Y
CVE-2026-1889	The Outgrow plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' attribute of the 'outgrow'...	Vulnerability via the 'id' attribute of the 'outgrow' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 2.1..	Patched by core rule	Y
CVE-2026-1886	The Go Night Pro | WordPress Dark Mode Plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plug...	This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-1854	The Post Flagger plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'flag' shortcode ...	Vulnerability via the plugin's 'flag' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.	Patched by core rule	Y
CVE-2026-1851	The iVysilani Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'width' shortcode a...	Vulnerability via the 'width' shortcode attribute due to insufficient input sanitization or output escaping. Affects versions up to and including 3.0.	Patched by core rule	Y
CVE-2026-1822	The WP NG Weather plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ng-weather' sho...	Vulnerability via the plugin's 'ng-weather' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.9.	Patched by core rule	Y
CVE-2026-1806	The Tour & Activity Operator Plugin for TourCMS plugin for WordPress is vulnerable to Stored Cross-Site Scripting via...	Vulnerability via the 'target' parameter of the tourcms_doc_link shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.7.0.	Patched by core rule	Y
CVE-2026-1647	The Comment Genius plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']...	Vulnerability via the `$_SERVER['PHP_SELF']` parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.5.	Patched by core rule	Y
CVE-2026-1575	The Schema Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `itemscope` s...	Vulnerability via the plugin's `itemscope` shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.	Patched by core rule	Y
CVE-2026-1397	The PQ Addons — Creative Elementor Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting	Vulnerability via widget attributes due to insufficient input sanitization or output escaping. Affects versions up to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	via widg...	and including 1.0.0.		
CVE-2026-1278	The Mandatory Field plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versi...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.6.8.	Patched by core rule	Y
CVE-2026-1275	The Multi Post Carousel by Category plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slides...	Vulnerability via the 'slides' shortcode attribute due to insufficient input sanitization or output escaping. Affects versions up to and including 1.4..	Patched by core rule	Y
CVE-2026-1247	The Survey plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.	Patched by core rule	Y
CVE-2026-1093	The WPFAQBlock— FAQ & Accordion Plugin For Gutenberg plugin for WordPress is vulnerable to Stored Cross-Site Scriptin...	Vulnerability via the 'class' parameter of the 'wpfaqblock' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.	Patched by core rule	Y
CVE-2026-0609	The Logo Slider — Logo Carousel, Logo Showcase & Client Logo Slider Plugin plugin for WordPress is vulnerable to Stor...	Vulnerability via the image alt text due to insufficient input sanitization or output escaping. Affects versions up to and including 4.9.0.	Patched by core rule	Y
CVE-2025-13910	The WP-WebAuthn plugin for WordPress is vulnerable to Unauthenticated Stored Cross-Site Scripting via the `wwa_auth` ...	Vulnerability via the `wwa_auth` AJAX endpoint due to insufficient input sanitization or output escaping. Affects versions up to and including 1.3.4.	Patched by core rule	Y
CVE-2026-4083	The Scoreboard for HTML5 Games Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'scoreb...	Vulnerability via the 'scoreboard' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2..	Patched by core rule	Y
CVE-2026-3577	The Keep Backup Daily plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the backup title alias (`...	Vulnerability via the backup title alias (`val` parameter) in the `update_kbd_bkup_alias` AJAX action due to insufficient input sanitization or output escaping. Affects versions up to and including 2.1.2..	Patched by core rule	Y
CVE-2026-3572	The iTracker360 plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to Stored Cross-Site Scripti...	This is due to missing nonce verification on the settings form submission and insufficient input sanitization combined with missing output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts via a forged request granted they can trick an administrator into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2026-3516	The Contact List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the '_cl_map_iframe' parameter...	Vulnerability via the '_cl_map_iframe' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 3.0.18..	Patched by core rule	Y
CVE-2026-3368	The Injection Guard plugin for WordPress is vulnerable to Stored Cross-Site Scripting	Vulnerability via malicious query parameter names due to insufficient input sanitization or	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	via malicious query parameter n...	output escaping. Affects versions up to and including 1.2.9..		
CVE-2026-3350	The Image Alt Text Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post title in al...	Vulnerability via the post title due to insufficient input sanitization or output escaping. Affects versions up to and including 1.8.2..	Patched by core rule	Y
CVE-2026-2430	The Autoptimize plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the lazy-loading image processi...	Vulnerability via the lazy-loading image processing due to insufficient input sanitization or output escaping. Affects versions up to and including 3.1.14..	Patched by core rule	Y
CVE-2026-2352	The Autoptimize plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ao_post_preload' meta valu...	Vulnerability via the 'ao_post_preload' meta value due to insufficient input sanitization or output escaping. Affects versions up to and including 3.1.14..	Patched by core rule	Y
CVE-2026-33230	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting researc...	In versions 3.9.3 and prior, `nltk.app.wordnet_app` contains a reflected cross-site scripting issue in the `lookup_...` route. A crafted `lookup_<payload>` URL can inject arbitrary HTML/JavaScript into the response page because attacker-controlled `word` data is reflected into HTML without escaping. This impacts users running the local WordNet Browser server and can lead to script execution in the browser origin of that application.	Patched by core rule	Y
CVE-2026-33140	PySpector is a static analysis security testing (SAST) Framework engineered for modern Python development workflows.	PySpector versions 0.1.6 and prior are affected by a stored Cross-Site Scripting (XSS) vulnerability in the HTML report generator. When PySpector scans a Python file containing JavaScript payloads (i.e. inside a string passed to eval()), the flagged code snippet is interpolated into the HTML report without sanitization. Opening the generated report in a browser causes the embedded JavaScript to execute in the browser's local file context. This issue has been patched in version 0.1.7.	Patched by core rule	Y
CVE-2026-33136	WeGIA is a web manager for charitable institutions.	Versions 3.6.6 and below have a Reflected Cross-Site Scripting (XSS) vulnerability in the listar_memorandos_ativos.php endpoint. An attacker can inject arbitrary JavaScript or HTML tags into the sccd GET parameter, which is then directly echoed into the HTML response without any sanitization or encoding. The script /html/memorando/listar_memorandos_ativos.php handles dynamic success messages to users using query string parameters.	Patched by core rule	Y
CVE-2026-33135	WeGIA is a web manager for charitable institutions.	Versions 3.6.6 and below have a Reflected Cross-Site Scripting (XSS) vulnerability in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		novo_memorandoo.php endpoint. An attacker can inject arbitrary JavaScript into the sccs GET parameter, which is directly echoed into the HTML response without any sanitization or encoding. The script /html/memorando/novo_memorandoo.php reads HTTP GET parameters to display dynamic success messages to the user. At approximately line 273, the code checks if $_GET['msg'] equals 'success'.		
CVE-2024-31119	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Vasilis Triantafyl	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Vasilis Triantafyllou Special Box for Content allows DOM-Based XSS.This issue affects Special Box for Content: from n/a through 1.	Patched by core rule	Y
CVE-2026-33067	SiYuan is a personal knowledge management system.	Versions 3.6.0 and below render package metadata fields (displayName, description) using template literals without HTML escaping. A malicious package author can inject arbitrary HTML/JavaScript into these fields, which executes automatically when any user browses the Bazaar page.	Patched by core rule	Y
CVE-2026-33066	SiYuan is a personal knowledge management system.	In versions 3.6.0 and below, the backend renderREADME function uses lute.New() without calling SetSanitize(true), allowing raw HTML embedded in Markdown to pass through unmodified. The frontend then assigns the rendered HTML to innerHTML without any additional sanitization. A malicious package author can embed arbitrary JavaScript in their README that executes when a user clicks to view the package details.	Patched by core rule	Y
CVE-2026-2432	The CM Custom Reports — Flexible reporting to track what matters most plugin for WordPress is vulnerable to Stored Cr...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.7.	Patched by core rule	Y
CVE-2026-4474	itsourcecode University Management System — Cross-Site Scripting	This manipulation of the argument st_name causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-33035	WWBN AVideo is an open source video platform.	User input from a URL parameter flows through PHP's json_encode() into a JavaScript function that renders it via innerHTML, bypassing encoding and achieving full script execution. The vulnerability is caused by two issues working together: unescaped user input passed to JavaScript (videoNotFound.php), and innerHTML rendering HTML tags as executable DOM (script.js).	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-32940	SiYuan is a personal knowledge management system.	In versions 3.6.0 and below, SanitizeSVG has an incomplete blocklist — it blocks data:text/html and data:image/svg+xml in href attributes but misses data:text/xml and data:application/xml, both of which can render SVG with JavaScript execution. The unauthenticated /api/icon/getDynamicIcon endpoint serves user-controlled input (via the content parameter) directly into SVG markup using fmt.Sprintf with no escaping, served as Content-Type: image/svg+xml.	Patched by core rule	Y
CVE-2026-32880	ChurchCRM is an open-source church management system.	Versions prior to 7.0.2 allow an admin user to edit JSON type system settings to store a JavaScript payload that can execute when any admin views the system settings. The JSON input is left unescaped/unsanitized in SystemSettings.php, leading to XSS. This issue has been fixed in version 7.0.2.	Patched by core rule	Y
CVE-2026-32757	Admidio is an open-source user management solution.	In versions 5.0.6 and below, the eCard send handler uses a raw $_POST['ecard_message'] value instead of the HTMLPurifier-sanitized $formValues['ecard_message'] when constructing the greeting card HTML. This allows an authenticated attacker to inject arbitrary HTML and JavaScript into greeting card emails sent to other members, bypassing the server-side HTMLPurifier sanitization that is properly applied to the ecard_message field during form validation.	Patched by core rule	Y
CVE-2026-32754	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework.	Versions 1.8.208 and below are vulnerable to Stored Cross-Site Scripting (XSS) through FreeScout's email notification templates. Incoming email bodies are stored in the database without sanitization and rendered unescaped in outgoing email notifications using Blade's raw output syntax {!! $thread->body !!}.	Patched by core rule	Y
CVE-2026-32751	SiYuan is a personal knowledge management system.	In versions 3.6.0 and below, the mobile file tree (MobileFiles.ts) renders notebook names via innerHTML without HTML escaping when processing renamenotebook WebSocket events. The desktop version (Files.ts) properly uses escapeHtml() for the same operation. An authenticated user who can rename notebooks can inject arbitrary HTML/JavaScript that executes on any mobile client viewing the file tree.	Patched by core rule	Y
CVE-2026-32040	OpenClaw versions prior to 2026.2.23 contain an html	OpenClaw versions prior to 2026.2.23 contain an html	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection vulnerability in the HTML session exporter that allows...	injection vulnerability in the HTML session exporter that allows attackers to execute arbitrary javascript by injecting malicious mimeType values in image content blocks. Attackers can craft session entries with specially crafted mimeType attributes that break out of the img src data-URL context to achieve cross-site scripting when exported HTML is opened.		
CVE-2026-33346	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.2, a stored cross-site scripting (XSS) vulnerability in the patient portal payment flow allows a patient portal user to persist arbitrary JavaScript that executes in the browser of a staff member who reviews the payment submission. The payload is stored via `portal/lib/paylib.php` and rendered without escaping in `portal/portal_payment.php`. Version 8.0.0.2 fixes the issue.	Patched by core rule	Y
CVE-2026-33303	OpenEMR is a free and open source electronic health records and medical practice management application.	Versions prior to 8.0.0.2 are vulnerable to stored cross-site scripting (XSS) via unescaped `portal_login_username` in the portal credential print view. A patient portal user can set their login username to an XSS payload, which then executes in a clinic staff member's browser when they open the "Create Portal Login" page for that patient. This crosses from the patient session context into the staff/admin session context. Version 8.0.0.2 fixes the issue.	Patched by core rule	Y
CVE-2026-33299	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.2, users with the `Notes - my encounters` role can fill **Eye Exam** forms in patient encounters. The answers to the form are displayed on the encounter page and in the visit history for the users with the same role. There exists a stored cross-site scripting (XSS) vulnerability in the function to display the form answers, allowing any authenticated attacker with the specific role to insert arbitrary JavaScript into the system by entering malicious payloads to the form answers.	Patched by core rule	Y
CVE-2026-32119	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.2, DOM-based stored XSS in the jQuery SearchHighlight plugin (`library/js/SearchHighlight.js`) allows an authenticated user with encounter form write access to inject arbitrary JavaScript that executes in another clinician's browser session when they use the search/find feature on the Custom Report page.	Patched by core rule	Y
CVE-2026-27070	Everest Forms Pro — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPEverest	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Everest Forms Pro allows Stored XSS.This issue affects Everest Forms Pro: from n/a through 1.9.10.		
CVE-2026-27068	Website LLMs.Txt — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ryan Howard Website LLMs.Txt allows Reflected XSS.This issue affects Website LLMs.Txt: from n/a through 8.2.6.	Patched by core rule	Y
CVE-2026-25442	Kentha — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QantumThemes Kentha allows Reflected XSS.This issue affects Kentha: from n/a through 4.7.2.	Patched by core rule	Y
CVE-2026-25438	Gutenberg Blocks — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeHunk Gutenberg Blocks allows Reflected XSS.This issue affects Gutenberg Blocks: from n/a through 1.2.8.	Patched by core rule	Y
CVE-2025-68836	Table of Contents Creator — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Markbeljaars Table of Contents Creator allows Reflected XSS.This issue affects Table of Contents Creator: from n/a through 1.6.4.1.	Patched by core rule	Y
CVE-2025-67618	Brookside — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ArtstudioWorks Brookside allows Reflected XSS.This issue affects Brookside: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-62043	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in WPSight WPCasa all	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in WPSight WPCasa allows DOM-Based XSS.This issue affects WPCasa: from n/a through 1.4.1.	Patched by core rule	Y
CVE-2025-53222	tagDiv Opt-In Builder — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Opt-In Builder allows Reflected XSS.This issue affects tagDiv Opt-In Builder: from n/a through 1.7.3.	Patched by core rule	Y
CVE-2025-50001	tagDiv Composer — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer allows Reflected XSS.This issue affects tagDiv Composer: from n/a through 5.4.2.	Patched by core rule	Y
CVE-2026-4120	The Info Cards — Add Text and Media in Card Layouts plugin for WordPress is vulnerable to Stored Cross-Site Scripting...	Vulnerability via the 'btnUrl' parameter within the Info Cards block due to insufficient input sanitization or output escaping. Affects versions up to and including 2.0.7..	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-4006	The Simple Draft List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'display_name' post m...	Vulnerability via the 'display_name' post meta (Custom Field) due to insufficient input sanitization or output escaping. Affects versions up to and including 2.6.2..	Patched by core rule	Y
CVE-2026-28073	WP eMember — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tips and Tricks HQ WP eMember allows Reflected XSS.This issue affects WP eMember: from n/a through v10.2.2.	Patched by core rule	Y
CVE-2026-28044	WP Rocket — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Media WP Rocket allows Stored XSS.This issue affects WP Rocket: from n/a through 3.19.4.	Patched by core rule	Y
CVE-2026-1238	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fh' (fingerprint) p...	Vulnerability via the 'fh' (fingerprint) parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 5.3.5.	Patched by core rule	Y
CVE-2026-32722	Memray is a memory profiler for Python.	Prior to Memray 1.19.2, Memray rendered the command line of the tracked process directly into generated HTML reports without escaping. Because there was no escaping, attacker-controlled command line arguments were inserted as raw HTML into the generated report. This allowed JavaScript execution when a victim opened the generated report in a browser. Version 1.19.2 fixes the issue.	Patched by core rule	Y
CVE-2026-29859	An arbitrary file upload vulnerability in aaPanel v7.57.0 allows attackers to execute arbitrary code via uploading a ...	An arbitrary file upload vulnerability in aaPanel v7.57.0 allows attackers to execute arbitrary code via uploading a crafted file.	Patched by core rule	Y
CVE-2026-3090	The Post SMTP — Complete Email Deliverability and SMTP Solution with Email Logs, Alerts, Backup SMTP & Mobile App plu...	Vulnerability via the 'event_type' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 3.8.0.	Patched by core rule	Y
CVE-2026-2512	The Code Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom field meta values in all ...	Vulnerability via custom field meta values due to insufficient input sanitization or output escaping. Affects versions up to and including 2.5.1..	Patched by core rule	Y
CVE-2026-3512	The Writeprint Stylometry plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'p' GET parame...	Vulnerability via the 'p' GET parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 0.1..	Patched by core rule	Y
CVE-2025-15363	The Get Use APIs WordPress plugin before 2.0.10 executes imported JSON, which could allow users with a role as low as...	The Get Use APIs WordPress plugin before 2.0.10 executes imported JSON, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks under certain server configurations.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-1780	The [CR]Paid Link Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the URL path in al...	Vulnerability via the URL path due to insufficient input sanitization or output escaping. Affects versions up to and including 0.5.	Patched by core rule	Y
CVE-2026-4268	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'w...	Vulnerability via the 'wpgmza_custom_js' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 10.0.05.	Patched by core rule	Y
CVE-2026-28499	LeafKit is a templating language with Swift-inspired syntax.	Prior to version 1.14.2, HTML escaping doesn't work correctly when a template prints a collection (Array / Dictionary) via `#(value)`. This can result in XSS, allowing potentially untrusted input to be rendered unescaped. Version 1.14.2 fixes the issue.	Patched by core rule	Y
CVE-2025-57543	Cross Site scripting vulnerability (XSS) in NetBox 4.3.5 "comment" field on object forms.	Cross Site scripting vulnerability (XSS) in NetBox 4.3.5 "comment" field on object forms. An attacker can inject arbitrary HTML, which will be rendered in the web UI when viewed by other users. This could potentially lead to user interface redress attacks or be escalated to XSS in certain contexts.	Patched by core rule	Y
CVE-2026-25369	Flexmls® IDX — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Flexmls Flexmls® IDX allows Reflected XSS.This issue affects Flexmls® IDX: from n/a through 3.15.9.	Patched by core rule	Y
CVE-2026-32626	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during cha...	In 1.11.1 and earlier, AnythingLLM Desktop contains a Streaming Phase XSS vulnerability in the chat rendering pipeline that escalates to Remote Code Execution on the host OS due to insecure Electron configuration. This works with default settings and requires no user interaction beyond normal chat usage. The custom markdown-it image renderer in frontend/src/utils/chat/markdown.js interpolates token.content directly into the alt attribute without HTML entity escaping.	Patched by core rule	Y
CVE-2016-20036	Wowza Streaming Engine 4.5.0 contains multiple reflected cross-site scripting vulnerabilities in the enginemanager in...	Attackers can inject malicious script code through parameters like appName, vhost, uiAppType, and wowzaCloudDestinationType in multiple endpoints to execute arbitrary HTML and JavaScript in a user's browser session.	Patched by core rule	Y
CVE-2016-20032	ZKTeco ZKAccess Security System 5.3.1 contains a stored cross-site scripting vulnerability that allows attackers to e...	Attackers can submit crafted requests with script code in these parameters to compromise user browser sessions and steal sensitive information.	Patched by core rule	Y
CVE-2015-20119	Next Click Ventures RealtyScript 4.0.2 contains a	Attackers can submit POST requests to the add page action	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	stored cross-site scripting vulnerability that allows authenticated...	with crafted iframe payloads in the text parameter to store malicious content that executes in the browsers of users viewing the affected pages.		
CVE-2015-20118	Next Click Ventures RealtyScript 4.0.2 contains a stored cross-site scripting vulnerability in the location_name para...	Attackers can submit POST requests to the locations.php endpoint with JavaScript payloads in the location_name field to execute arbitrary code in administrator browsers.	Patched by core rule	Y
CVE-2015-20116	Next Click Ventures RealtyScript 4.0.2 fails to properly sanitize CSV file uploads, allowing attackers to inject mali...	Next Click Ventures RealtyScript 4.0.2 fails to properly sanitize CSV file uploads, allowing attackers to inject malicious scripts through filename parameters in multipart form data. Attackers can upload files with XSS payloads in the filename field to execute arbitrary JavaScript in users' browsers when the file is processed or displayed.	Patched by core rule	Y
CVE-2015-20115	Next Click Ventures RealtyScript 4.0.2 fails to properly sanitize file uploads, allowing attackers to store malicious...	Next Click Ventures RealtyScript 4.0.2 fails to properly sanitize file uploads, allowing attackers to store malicious scripts through the file POST parameter in admin/tools.php. Attackers can upload files containing JavaScript code that executes in the context of admin/tools.php when accessed by other users.	Patched by core rule	Y
CVE-2015-20114	Next Click Ventures RealtyScript 4.0.2 contains a cross-site scripting vulnerability that allows attackers to execute...	Attackers can craft requests with injected script payloads in vulnerable parameters to execute code in users' browser sessions within the context of the affected application.	Patched by core rule	Y
CVE-2013-20006	Qool CMS contains multiple persistent cross-site scripting vulnerabilities in several administrative scripts where PO...	Attackers can inject malicious JavaScript code through parameters like 'title', 'name', 'email', 'username', 'link', and 'task' in endpoints such as addnewtype, addnewdatafield, addmenu, addusergroup, addnewuserfield, adduser, addgeneraldata, and addcontentitem to execute arbitrary scripts in administrator browsers.	Patched by core rule	Y
CVE-2013-20005	Qool CMS 2.0 RC2 contains a cross-site request forgery vulnerability that allows attackers to perform administrative ...	Attackers can forge POST requests to the /admin/adduser endpoint with parameters like username, password, email, and level to create root-level user accounts without user consent.	Patched by core rule	Y
CVE-2026-3986	The Calculated Fields Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form settings in...	Vulnerability via the form settings due to insufficient input sanitization or output escaping. Affects versions up to and including 5.4.5.0..	Patched by core rule	Y
CVE-2026-32612	Statamic is a Laravel and Git powered content management system (CMS).	Prior to 6.6.2, stored XSS in the control panel color mode preference allows authenticated users with control panel access to inject malicious JavaScript that executes when a higher-privileged user impersonates their account. This has been fixed in 6.6.2.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-32462	Master Addons for Elementor — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liton Arefin Master Addons for Elementor master-addons allows DOM-Based XSS.This issue affects Master Addons for Elementor: from n/a through <= 2.1.3.	Patched by core rule	Y
CVE-2026-32460	Ultimate Addons for Contact Form 7 — Exploiting Incorrectly Configured Access Control Security Levels	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Ultimate Addons for Contact Form 7 ultimate-addons-for-contact-form-7 allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ultimate Addons for Contact Form 7: from n/a through <= 3.5.36.	Patched by core rule	Y
CVE-2026-32455	MDTF — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 MDTF wp-meta-data-filter-and-taxonomy-filter allows DOM-Based XSS.This issue affects MDTF: from n/a through <= 1.3.5.	Patched by core rule	Y
CVE-2026-32454	Avada Core — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeFusion Avada Core fusion-core allows DOM-Based XSS.This issue affects Avada Core: from n/a through < 5.15.0.	Patched by core rule	Y
CVE-2026-32450	Active Products Tables for WooCommerce — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 Active Products Tables for WooCommerce profit-products-tables-for-woocommerce allows DOM-Based XSS.This issue affects Active Products Tables for WooCommerce: from n/a through <= 1.0.7.	Patched by core rule	Y
CVE-2026-32449	Themify Event Post — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Event Post themify-event-post allows Stored XSS.This issue affects Themify Event Post: from n/a through <= 1.3.4.	Patched by core rule	Y
CVE-2026-32448	Podlove Podcast Publisher — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eric Teubert Podlove Podcast Publisher podlove-podcasting-plugin-for-wordpress allows Stored XSS.This issue affects Podlove Podcast Publisher: from n/a through <= 4.3.3.	Patched by core rule	Y
CVE-2026-32431	Astra Bulk Edit — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability in Brainstorm Force Astra Bulk Edit astra-bulk-edit allows DOM-Based XSS.This issue affects Astra Bulk Edit: from n/a through <= 1.2.10.		
CVE-2026-32430	PowerPack Addons for Elementor — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IdeaBox Creations PowerPack Addons for Elementor powerpack-lite-for-elementor allows Stored XSS.This issue affects PowerPack Addons for Elementor: from n/a through <= 2.9.9.	Patched by core rule	Y
CVE-2026-32429	Magical Addons For Elementor — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor Alam Magical Addons For Elementor magical-addons-for-elementor allows Stored XSS.This issue affects Magical Addons For Elementor: from n/a through <= 1.4.1.	Patched by core rule	Y
CVE-2026-32424	Sprout Clients — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldGrid Sprout Clients sprout-clients allows Stored XSS.This issue affects Sprout Clients: from n/a through <= 3.2.2.	Patched by core rule	Y
CVE-2026-32419	List category posts — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fernando Briano List category posts list-category-posts allows DOM-Based XSS.This issue affects List category posts: from n/a through <= 0.93.1.	Patched by core rule	Y
CVE-2026-32411	Embed Calendly — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Simpma Embed Calendly embed-calendly-scheduling allows Stored XSS.This issue affects Embed Calendly: from n/a through <= 4.4.	Patched by core rule	Y
CVE-2026-32403	Toocheke Companion — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in toocheke Toocheke Companion toocheke-companion allows DOM-Based XSS.This issue affects Toocheke Companion: from n/a through <= 1.194.	Patched by core rule	Y
CVE-2026-32361	Editorial Calendar — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marketing Fire Editorial Calendar editorial-calendar allows DOM-Based XSS.This issue affects Editorial Calendar: from n/a through <= 3.9.0.	Patched by core rule	Y
CVE-2026-32360	Rich Showcase for Google Reviews — Stored XSS	Improper Neutralization of Input During Web Page Generation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		('Cross-site Scripting') vulnerability in richplugins Rich Showcase for Google Reviews widget-google-reviews allows Stored XSS.This issue affects Rich Showcase for Google Reviews: from n/a through <= 6.9.4.3.		
CVE-2026-32359	Icon List Block — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Icon List Block icon-list-block allows Stored XSS.This issue affects Icon List Block: from n/a through <= 1.2.3.	Patched by core rule	Y
CVE-2026-32356	Robo Gallery — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in robosoft Robo Gallery robo-gallery allows DOM-Based XSS.This issue affects Robo Gallery: from n/a through <= 5.1.2.	Patched by core rule	Y
CVE-2026-32352	Elementor Website Builder — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elementor Elementor Website Builder elementor allows DOM-Based XSS.This issue affects Elementor Website Builder: from n/a through <= 3.35.5.	Patched by core rule	Y
CVE-2026-32351	PowerPress Podcasting — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in blubrry PowerPress Podcasting powerpress allows Stored XSS.This issue affects PowerPress Podcasting: from n/a through <= 11.15.13.	Patched by core rule	Y
CVE-2026-32308	OneUptime is a solution for monitoring and managing online services.	Prior to 10.0.23, the Markdown viewer component renders Mermaid diagrams with securityLevel: "loose" and injects the SVG output via innerHTML. This configuration explicitly allows interactive event bindings in Mermaid diagrams, enabling XSS through Mermaid's click directive which can execute arbitrary JavaScript. Any field that renders markdown (incident descriptions, status page announcements, monitor notes) is vulnerable. This vulnerability is fixed in 10.0.23.	Patched by core rule	Y
CVE-2026-31918	immonex Kickstart — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in immonex immonex Kickstart immonex-kickstart allows Stored XSS.This issue affects immonex Kickstart: from n/a through <= 1.13.0.	Patched by core rule	Y
CVE-2026-22210	wpDiscuz before 7.6.47 contains a cross-site scripting vulnerability that allows attackers to inject malicious code t...	Attackers can craft malicious attachment records or filter hooks to inject arbitrary JavaScript into img and anchor tag attributes, executing code in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the context of WordPress users viewing comments.		
CVE-2026-32139	Dataease is an open source data visualization analysis tool.	In DataEase 2.10.19 and earlier, the static resource upload interface allows SVG uploads. However, backend validation only checks whether the XML is parseable and whether the root node is svg. It does not sanitize active content such as onload/onerror event handlers or script-capable attributes. As a result, an attacker can upload a malicious SVG and then trigger script execution in a browser by visiting the exposed static resource URL, forming a full stored XSS exploitation chain.	Patched by core rule	Y
CVE-2026-31873	Unhead is a document head and template manager.	Prior to 2.1.11, The link.href check in makeTagSafe (safe.ts) uses String.includes(), which is case-sensitive. Browsers treat URI schemes case-insensitively. DATA:text/css,... is the same as data:text/css,... to the browser, but 'DATA:...'.includes('data:') returns false. An attacker can inject arbitrary CSS for UI redressing or data exfiltration via CSS attribute selectors with background-image callbacks. This vulnerability is fixed in 2.1.11.	Patched by core rule	Y
CVE-2026-31860	Unhead is a document head and template manager.	Prior to 2.1.11, useHeadSafe() can be bypassed to inject arbitrary HTML attributes, including event handlers, into SSR-rendered <head> tags. This is the composable that Nuxt docs recommend for safely handling user-generated content. The acceptDataAttrs function (safe.ts, line 16-20) allows any property key starting with data- through to the final HTML. It only checks the prefix, not whether the key contains spaces or other characters that break HTML attribute parsing.	Patched by core rule	Y
CVE-2026-2987	The Simple Ajax Chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'c' parameter in versi...	This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-2687	The Reading progressbar WordPress plugin before 1.3.1 does not sanitise and escape some of its settings, which could ...	The Reading progressbar WordPress plugin before 1.3.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	Patched by core rule	Y
CVE-2026-32125	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.1, track/item names from the Track Anything feature are stored from user input (POST) and later rendered in Dygraph charts (titles/labels) using innerHTML or equivalent without escaping. A user who can create or edit Track	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Anything items can inject script that runs when any user views the corresponding graph. This vulnerability is fixed in 8.0.0.1.		
CVE-2026-32124	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.1, the dynamic code picker AJAX endpoint returns code descriptions (code_text) that are rendered in the front end (e.g. DataTables) without HTML escaping. If an administrator (or user with code management rights) creates or edits a code with a malicious description containing script, that script runs in the browser of every user who uses the picker. This vulnerability is fixed in 8.0.0.1.	Patched by core rule	Y
CVE-2026-32121	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.1, Stored XSS in prescription CSS/HTML print view via patient demographics. That finding involves server-side rendering of patient names via raw PHP echo. This finding involves client-side DOM-based rendering via jQuery .html() in a completely different component (portal/sign/assets/signer_api.js).	Patched by core rule	Y
CVE-2026-32118	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to 8.0.0.1, stored cross-site scripting (XSS) in the Graphical Pain Map ("clickmap") form allows any authenticated clinician to inject arbitrary JavaScript that executes in the browser of every subsequent user who views the affected encounter form. Because session cookies are not marked HttpOnly, this enables full session hijacking of other users, including administrators. This vulnerability is fixed in 8.0.0.1.	Patched by core rule	Y
CVE-2026-3178	The Name Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name_directory_name' pa...	Vulnerability via the 'name_directory_name' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.32.1.	Patched by core rule	Y
CVE-2026-3492	The Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and includ...	This is due to a compound failure involving missing authorization on the `create_from_template` AJAX endpoint (allowing any authenticated user to create forms), insufficient input sanitization (`sanitize_text_field()` preserves single quotes), and missing output escaping when the form title is rendered in the Form Switcher dropdown (`title` attribute constructed without `esc_attr()`, and JavaScript `saferHtml` utility only escapes `&`, `<`, `>` but not quotes).	Patched by core rule	Y
CVE-2026-3231	The Checkout Field Editor (Checkout Manager) for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site ...	Vulnerability via custom radio and checkboxgroup field values submitted through the WooCommerce Block Checkout Store API due to insufficient input sanitization or output escaping. Affects versions up to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and including 2.1.7..		
CVE-2026-1454	The Responsive Contact Form Builder & Lead Generation Plugin plugin for WordPress is vulnerable to Stored Cross-Site ...	This is due to insufficient input sanitization in the lfb_lead_sanitize() function which omits certain field types from its sanitization whitelist, combined with an overly permissive wp_kses() filter at output time that allows onclick attributes on anchor tags. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator views the lead entries in the WordPress dashboard.	Patched by core rule	Y
CVE-2026-3534	The Astra theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `ast-page-background-meta` and `as...	This is due to insufficient input sanitization on meta registration and missing output escaping in the `astra_get_responsive_background_obj()` function for four CSS-context sub-properties (`background-color`, `background-image`, `overlay-color`, `overlay-gradient`). This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-2707	The weForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the REST API entry submission endpo...	Vulnerability via the REST API entry submission endpoint due to insufficient input sanitization or output escaping. Affects versions up to and including 1.6.27..	Patched by core rule	Y
CVE-2026-2466	The DukaPress WordPress plugin through 3.2.4 does not sanitise and escape a parameter before outputting it back in th...	The DukaPress WordPress plugin through 3.2.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	Patched by core rule	Y
CVE-2026-2358	The WP ULike plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `[wp_ulike_likers_box]` shortc...	Vulnerability via the `[wp_ulike_likers_box]` shortcode `template` attribute due to insufficient input sanitization or output escaping. Affects versions up to and including 5.0.1..	Patched by core rule	Y
CVE-2025-12473	The RTMKit plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'themebuilder' parameter in a...	Vulnerability via the 'themebuilder' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.6.8.	Patched by core rule	Y
CVE-2026-2569	The Dear Flipbook — PDF Flipbook, 3D Flipbook, PDF embed, PDF viewer plugin for WordPress is vulnerable to Stored Cro...	Vulnerability via PDF page labels due to insufficient input sanitization or output escaping. Affects versions up to and including 2.4.20.	Patched by core rule	Y
CVE-2026-31809	SiYuan is a personal knowledge management system.	Prior to 3.5.10, SiYuan's SVG sanitizer (SanitizeSVG) checks href attributes for the javascript: prefix using strings.HasPrefix().	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		However, inserting ASCII tab ( ), newline (
), or carriage return (
) characters inside the javascript: string bypasses this prefix check. Browsers strip these characters per the WHATWG URL specification before parsing the URL scheme, so the JavaScript still executes.		
CVE-2026-31807	SiYuan is a personal knowledge management system.	Prior to 3.5.10, SiYuan's SVG sanitizer (SanitizeSVG) blocks dangerous elements (<script>, <iframe>, <foreignobject>) and removes on* event handlers and javascript: in href attributes. However, it does NOT block SVG animation elements (<animate>, <set>) which can dynamically set attributes to dangerous values at runtime, bypassing the static sanitization.	Patched by core rule	Y
CVE-2026-29177	Craft Commerce is an ecommerce platform for Craft CMS.	Prior to 4.10.2 and 5.5.3, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Craft Commerce Order details. Malicious JavaScript can be injected via the Shipping Method Name, Order Reference, or Site Name. When a user opens the order details slideout via a double-click on the order index page, the injected payload executes. This vulnerability is fixed in 4.10.2 and 5.5.3.	Patched by core rule	Y
CVE-2026-29175	Craft Commerce is an ecommerce platform for Craft CMS.	Prior to 5.5.3, Stored XSS vulnerabilities exist in the Commerce Inventory page. The Product Title, Variant Title, and Variant SKU fields are rendered without proper HTML escaping, allowing an attacker to execute arbitrary JavaScript when any user (including administrators) views the inventory management page. This vulnerability is fixed in 5.5.3.	Patched by core rule	Y
CVE-2026-29173	Craft Commerce is an ecommerce platform for Craft CMS.	Prior to 4.10.2 and 5.5.3, a stored XSS vulnerability exists when a user tries to update the Order Status from the Commerce Orders Table. The Order Status Name is rendered without proper escaping, allowing script execution to occur. This vulnerability is fixed in 4.10.2 and 5.5.3.	Patched by core rule	Y
CVE-2026-3228	The NextScripts: Social Networks Auto-Poster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th...	Vulnerability via the `[nxs_fbembed]` shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 4.4.6..	Patched by core rule	Y
CVE-2026-30934	FileBrowser Quantum is a free, self-hosted, web-based file manager.	Prior to 1.3.1-beta and 1.2.2-stable, Stored XSS is possible via share metadata fields (e.g., title, description) that are rendered into HTML for /public/share/<hash> without context-aware escaping. The server uses text/template instead of html/template,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allowing injected scripts to execute when victims visit the share URL. This vulnerability is fixed in 1.3.1-beta and 1.2.2-stable.		
CVE-2026-2724	The Unlimited Elements for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form e...	Vulnerability via the form entry fields due to insufficient input sanitization or output escaping. Affects versions up to and including 2.0.5..	Patched by core rule	Y
CVE-2026-1261	The MetForm Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Quiz feature in all version...	Vulnerability via the Quiz feature due to insufficient input sanitization or output escaping. Affects versions up to and including 3.9.6.	Patched by core rule	Y
CVE-2026-30919	facileManager is a modular suite of web apps built with the sysadmin in mind.	Prior to 6.0.4 , stored XSS (also known as persistent or second-order XSS) occurs when an application receives data from an untrusted source and includes that data in its subsequent HTTP responses in an unsafe manner. This vulnerability was found in the fmDNS module. This vulnerability is fixed in 6.0.4.	Patched by core rule	Y
CVE-2026-30918	facileManager is a modular suite of web apps built with the sysadmin in mind.	Prior to 6.0.4 , a reflected XSS occurs when an application receives data from an untrusted source and uses it in its HTTP responses in a way that could lead to vulnerabilities. It is possible to inject malicious JavaScript code into a URL by adding a script in a parameter. This vulnerability was found in the fmDNS module. The parameter that is vulnerable to an XSS attack is log_search_query. This vulnerability is fixed in 6.0.4.	Patched by core rule	Y
CVE-2026-30862	Appsmith is a platform to build admin panels, internal tools, and dashboards.	Prior to 1.96, a Critical Stored XSS vulnerability exists in the Table Widget (TableWidgetV2). The root cause is a lack of HTML sanitization in the React component rendering pipeline, allowing malicious attributes to be interpolated into the DOM. By leveraging the "Invite Users" feature, an attacker with a regular user account (user@gmail.com) can force a System Administrator to execute a high-privileged API call (/api/v1/admin/env), resulting in a Full Administrative Account Takeover.	Patched by core rule	Y
CVE-2026-25737	Budibase is a low code platform for creating internal tools, workflows, and admin panels.	In 3.24.0 and earlier, an arbitrary file upload vulnerability exists even though file extension restrictions are configured. The restriction is enforced only at the UI level. An attacker can bypass these restrictions and upload malicious files.	Patched by core rule	Y
CVE-2026-3819	SourceCodester Resort Reservation System — Cross-Site Scripting	Such manipulation of the argument ID leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and may be used.		
CVE-2026-3812	itsourcecode Payroll Management System — Cross-Site Scripting	Affected is an unknown function of the file /manage_employee_allowances.php. This manipulation of the argument ID causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-3766	SourceCodester Web-based Pharmacy Product Management System — Cross-Site Scripting	Performing a manipulation of the argument fullname results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-3763	code-projects Simple Flight Ticket Booking System — Cross-Site Scripting	The affected element is an unknown function of the file showhistory.php. The manipulation results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3743	YiFang CMS — Cross-Site Scripting	Executing a manipulation of the argument Name can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3742	YiFang CMS — Cross-Site Scripting	The impacted element is the function update of the file app/db/admin/D_singlePage.php. Performing a manipulation of the argument Title results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3741	YiFang CMS — Cross-Site Scripting	Such manipulation of the argument linkName leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3721	1024-lab/lab1024 SmartAdmin up to — Cross-Site Scripting	This manipulation causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3720	1024-lab/lab1024 SmartAdmin up to — Cross-Site Scripting	The manipulation results in cross site scripting. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		contacted early about this disclosure but did not respond in any way.		
CVE-2026-3716	Wavlink WL-WN579X3-C — Cross-Site Scripting	This vulnerability affects the function sub_401AD4 of the file /cgi-bin/adm.cgi. Executing a manipulation of the argument Hostname can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 20260226 is able to resolve this issue. The affected component should be upgraded.	Patched by core rule	Y
CVE-2026-3702	SourceCodester Loan Management System — Cross-Site Scripting	Affected by this issue is some unknown functionality of the file /index.php. Performing a manipulation of the argument page results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-2433	The RSS Aggregator — RSS Import, News Feeds, Feed to Post, and Autoblogging plugin for WordPress is vulnerable to DOM...	Vulnerability via postMessage due to insufficient input sanitization or output escaping. Affects versions up to and including 5.0.11..	Patched by core rule	Y
CVE-2026-2420	The LotekMedia Popup Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings i...	Vulnerability via the plugin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.6.	Patched by core rule	Y
CVE-2026-1825	The Show YouTube video plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'syv' short...	Vulnerability via the plugin's 'syv' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.	Patched by core rule	Y
CVE-2026-1824	The Infomaniak Connect for OpenID plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'endpoint...	Vulnerability via the 'endpoint_login' parameter of the infomaniak_connect_generic_auth_url shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.2.	Patched by core rule	Y
CVE-2026-1823	The Consensus Embed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's consensus shor...	Vulnerability via the plugin's consensus shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.6.	Patched by core rule	Y
CVE-2026-1820	The Media Library Alt Text Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ...	Vulnerability via the plugin's 'bvmalt_sc_div_update_alt_text' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.0.	Patched by core rule	Y
CVE-2026-1805	The DA Media GigList plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's damedia_gigli...	Vulnerability via the plugin's damedia_giglist shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.9.0.	Patched by core rule	Y
CVE-2026-1574	The MyQtip — easy qTip2 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `myqtip` s...	Vulnerability via the plugin's `myqtip` shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		2.0.5.		
CVE-2026-1569	The Wueen plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `wueen-blocket` shortcod...	Vulnerability via the plugin's `wueen-blocket` shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 0.2.0.	Patched by core rule	Y
CVE-2026-1074	The WP App Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'app-bar-features' parameter...	Vulnerability via the 'app-bar-features' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.5..	Patched by core rule	Y
CVE-2026-1071	The Carta Online plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 2.13.0.	Patched by core rule	Y
CVE-2026-30841	Wallos is an open-source, self-hostable personal subscription tracker.	Prior to version 4.6.2, passwordreset.php outputs $_GET["token"] and $_GET["email"] directly into HTML input value attributes using <?= $token ?> and <?= $email ?> without calling htmlspecialchars(). This allows reflected XSS by breaking out of the attribute context. This issue has been patched in version 4.6.2.	Patched by core rule	Y
CVE-2026-30830	Defuddle cleans up HTML pages.	Defuddle cleans up HTML pages. Prior to version 0.9.0, the _findContentBySchemaText method in src/defuddle.ts interpolates image src and alt attributes directly into an HTML string without escaping. An attacker can use a " in the alt attribute to break out of the attribute context and inject event handler. This issue has been patched in version 0.9.0.	Patched by core rule	Y
CVE-2026-2722	The Stock Ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 3.26.1.	Patched by core rule	Y
CVE-2026-2721	The MailArchiver plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 4.4.0.	Patched by core rule	Y
CVE-2026-2431	The CM Custom Reports plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'date_from' and 'd...	Vulnerability via the 'date_from' and 'date_to' parameters due to insufficient input sanitization or output escaping. Affects versions up to and including 1.2.7.	Patched by core rule	Y
CVE-2026-1902	The Hammas Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'apix' parameter in the...	Vulnerability via the 'apix' parameter in the 'hp-calendar-manage-redirect' shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.5.11.	Patched by core rule	Y
CVE-2026-30238	Group-Office is an enterprise customer relationship management and groupware tool.	Prior to versions 6.8.155, 25.0.88, and 26.0.10, there is a reflected XSS vulnerability in GroupOffice on the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		external/index flow. The f parameter (Base64 JSON) is decoded and then injected into an inline JavaScript block without strict escaping, allowing </script><script>...</script> injection and arbitrary JavaScript execution in the victim's browser. This issue has been patched in versions 6.8.155, 25.0.88, and 26.0.10.		
CVE-2026-30237	Group-Office is an enterprise customer relationship management and groupware tool.	Prior to versions 6.8.155, 25.0.88, and 26.0.10, there is a reflected XSS vulnerability in the GroupOffice installer, endpoint install/license.php. The POST field license is rendered without escaping inside a <textarea>, allowing a </textarea><script>...</script> breakout.. This issue has been patched in versions 6.8.155, 25.0.88, and 26.0.10.	Patched by core rule	Y
CVE-2026-29082	Kestra is an event-driven orchestration platform.	In versions from 1.1.10 and prior, Kestra's execution-file preview renders user-supplied Markdown (.md) with markdown-it instantiated as html:true and injects the resulting HTML with Vue's v-html without sanitisation. At time of publication, there are no publicly available patches.	Patched by core rule	Y
CVE-2024-35644	Preferred Languages — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pascal Birchler Preferred Languages allows DOM-Based XSS.This issue affects Preferred Languages: from n/a through 2.2.2.	Patched by core rule	Y
CVE-2026-29183	SiYuan is a personal knowledge management system.	Prior to version 3.5.9, an unauthenticated reflected XSS vulnerability exists in the dynamic icon API endpoint "GET /api/icon/getDynamicIcon" when type=8, attacker-controlled content is embedded into SVG output without escaping. Because the endpoint is unauthenticated and returns image/svg+xml, a crafted URL can inject executable SVG/HTML event handlers (for example onerror) and run JavaScript in the SiYuan web origin.	Patched by core rule	Y
CVE-2026-29038	changedetection.io is a free open source web page change detection tool.	Prior to version 0.54.4, there is a reflected cross-site scripting (XSS) vulnerability identified in the /rss/tag/ endpoint of changedetection.io. The tag_uuid path parameter is reflected directly in the HTTP response body without HTML escaping. Since Flask returns text/html by default for plain string responses, the browser parses and executes injected JavaScript. This issue has been patched in version 0.54.4.	Patched by core rule	Y
CVE-2026-28509	LangBot is a global IM bot platform designed for LLMs.	Prior to version 4.8.7, LangBot's web UI renders user-supplied raw HTML using rehypeRaw,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		which can lead to a cross-site scripting (XSS) vulnerability. This issue has been patched in version 4.8.7.		
CVE-2026-27605	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to creat...	Prior to version 4.8.4, the application allows uploading files (project logos) without validating the file type or content. It trusts the extension provided by the user. These files are saved to the uploads/ directory and served statically. An attacker can upload an HTML file containing malicious JavaScript. Since authentication tokens are likely stored in localStorage (as they are returned in the API body), this XSS can lead to account takeover. This issue has been patched in version 4.8.4.	Patched by core rule	Y
CVE-2026-2593	The Greenshift — animation and page builder blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting ...	Vulnerability via the `_gspb_post_css` post meta value and the `dynamicAttributes` block attribute due to insufficient input sanitization or output escaping. Affects versions up to and including 12.8.5.	Patched by core rule	Y
CVE-2026-26022	Gogs is an open source self-hosted Git service.	Prior to version 0.14.2, a stored cross-site scripting (XSS) vulnerability exists in the comment and issue description functionality. The application's HTML sanitizer explicitly allows data: URI schemes, enabling authenticated users to inject arbitrary JavaScript execution via malicious links. This issue has been patched in version 0.14.2.	Patched by core rule	Y
CVE-2026-26377	Cross Site Scripting vulnerability in Koha 25.11 and before allows a remote attacker to execute arbitrary code via th...	Cross Site Scripting vulnerability in Koha 25.11 and before allows a remote attacker to execute arbitrary code via the News function.	Patched by core rule	Y
CVE-2026-28137	MediCenter - Health Medical Clinic — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuanticaLabs MediCenter - Health Medical Clinic medicenter allows Reflected XSS.This issue affects MediCenter - Health Medical Clinic: from n/a through <= 14.9.	Patched by core rule	Y
CVE-2026-28130	UDesign — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AndonDesign UDesign u-design allows Reflected XSS.This issue affects UDesign: from n/a through <= 4.14.0.	Patched by core rule	Y
CVE-2026-28127	Lawyer Directory — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Lawyer Directory lawyer-directory allows Reflected XSS.This issue affects Lawyer Directory: from n/a through <= 1.3.2.	Patched by core rule	Y
CVE-2026-28126	RH Frontend Publishing Pro	Improper Neutralization of Input	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	— Reflected XSS	During Web Page Generation ('Cross-site Scripting') vulnerability in Sizam RH Frontend Publishing Pro allows Reflected XSS.This issue affects RH Frontend Publishing Pro: from n/a before 4.3.4.	rule	
CVE-2026-28122	ListingPro — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CridioStudio ListingPro listingpro-plugin allows Reflected XSS.This issue affects ListingPro: from n/a through <= 2.9.8.	Patched by core rule	Y
CVE-2026-28113	Ultimate Learning Pro — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in azzaroco Ultimate Learning Pro indeed-learning-pro allows Reflected XSS.This issue affects Ultimate Learning Pro: from n/a through <= 3.9.1.	Patched by core rule	Y
CVE-2026-28112	AllInOne - Banner Rotator — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup AllInOne - Banner Rotator all-in-one-bannerRotator allows Reflected XSS.This issue affects AllInOne - Banner Rotator: from n/a through <= 3.8.	Patched by core rule	Y
CVE-2026-28110	LambertGroup - AllInOne - Banner with Playlist — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Playlist all-in-one-bannerWithPlaylist allows Reflected XSS.This issue affects LambertGroup - AllInOne - Banner with Playlist: from n/a through <= 3.8.	Patched by core rule	Y
CVE-2026-28109	LambertGroup - AllInOne - Content Slider — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup LambertGroup - AllInOne - Content Slider all-in-one-contentSlider allows Reflected XSS.This issue affects LambertGroup - AllInOne - Content Slider: from n/a through <= 3.8.	Patched by core rule	Y
CVE-2026-28108	LambertGroup - AllInOne - Banner with Thumbnails — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup LambertGroup - AllInOne - Banner with Thumbnails all-in-one-thumbnailsBanner allows Reflected XSS.This issue affects LambertGroup - AllInOne - Banner with Thumbnails: from n/a through <= 3.8.	Patched by core rule	Y
CVE-2026-28103	LBG Zoominoutslider — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup LBG Zoominoutslider lbg_zoominoutslider allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Reflected XSS.This issue affects LBG Zoominoutslider: from n/a through <= 5.4.5.		
CVE-2026-28102	UberSlider Classic — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup UberSlider Classic uberSlider_classic allows Reflected XSS.This issue affects UberSlider Classic: from n/a through <= 2.5.	Patched by core rule	Y
CVE-2026-28101	UberSlider MouseInteraction — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup UberSlider MouseInteraction uberSlider_mouseinteraction allows Reflected XSS.This issue affects UberSlider MouseInteraction: from n/a through <= 2.3.	Patched by core rule	Y
CVE-2026-28100	UberSlider PerpetuumMobile — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup UberSlider PerpetuumMobile uberSlider_perpetuummobile allows Reflected XSS.This issue affects UberSlider PerpetuumMobile: from n/a through <= 2.3.	Patched by core rule	Y
CVE-2026-28099	UberSlider Ultra — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup UberSlider Ultra uberSlider_ultra allows Reflected XSS.This issue affects UberSlider Ultra: from n/a through <= 2.3.	Patched by core rule	Y
CVE-2026-28075	Porto — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in p-themes Porto porto allows Reflected XSS.This issue affects Porto: from n/a through <= 7.6.2.	Patched by core rule	Y
CVE-2026-28072	pixfort Core — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PixFort pixfort Core pixfort-core allows Reflected XSS.This issue affects pixfort Core: from n/a through <= 3.2.22.	Patched by core rule	Y
CVE-2026-28042	Listify — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Astoundify Listify listify allows Reflected XSS.This issue affects Listify: from n/a through <= 3.2.5.	Patched by core rule	Y
CVE-2026-28037	EventON — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ashanjay EventON eventon allows Reflected XSS.This issue affects EventON: from n/a through <= 4.9.12.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-27385	DesignThemes Portfolio — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designthemes DesignThemes Portfolio designthemes-portfolio allows Reflected XSS.This issue affects DesignThemes Portfolio: from n/a through <= 1.3.	Patched by core rule	Y
CVE-2026-27382	Metro — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RadiusTheme Metro metro allows DOM-Based XSS.This issue affects Metro: from n/a through <= 2.13.	Patched by core rule	Y
CVE-2026-27376	Claue - Clean, Minimal Elementor WooCommerce Theme — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JanStudio Claue - Clean, Minimal Elementor WooCommerce Theme claue allows Reflected XSS.This issue affects Claue - Clean, Minimal Elementor WooCommerce Theme: from n/a through <= 2.2.7.	Patched by core rule	Y
CVE-2026-27375	Gecko — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JanStudio Gecko gecko allows Reflected XSS.This issue affects Gecko: from n/a through <= 1.9.8.	Patched by core rule	Y
CVE-2026-27367	Musico — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Musico musico allows Reflected XSS.This issue affects Musico: from n/a through <= 3.2.4.	Patched by core rule	Y
CVE-2026-27363	WP Bakery Autoresponder Addon — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kamleshyadav WP Bakery Autoresponder Addon vc-autoresponder-addon allows Stored XSS.This issue affects WP Bakery Autoresponder Addon: from n/a through <= 1.0.6.	Patched by core rule	Y
CVE-2026-27359	Awa Plugins — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fox-themes Awa Plugins awa-plugins allows Reflected XSS.This issue affects Awa Plugins: from n/a through <= 1.4.4.	Patched by core rule	Y
CVE-2026-27358	Architecturer — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Architecturer architecturer allows Reflected XSS.This issue affects Architecturer: from n/a through <= 3.8.8.	Patched by core rule	Y
CVE-2026-27354	WooCommerce Coming Soon Product with Countdown — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebCodingPlace	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		WooCommerce Coming Soon Product with Countdown woo-coming-soon-product allows Stored XSS.This issue affects WooCommerce Coming Soon Product with Countdown: from n/a through <= 5.0.		
CVE-2026-27353	Grand News — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand News grandnews allows Reflected XSS.This issue affects Grand News: from n/a through <= 3.4.3.	Patched by core rule	Y
CVE-2026-27352	Starto — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Starto starto allows Reflected XSS.This issue affects Starto: from n/a through <= 2.1.9.	Patched by core rule	Y
CVE-2026-27348	Photography — DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Photography photography allows DOM-Based XSS.This issue affects Photography: from n/a through <= 7.6.1.	Patched by core rule	Y
CVE-2026-27332	Agrofood — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Skygroup Agrofood allows Reflected XSS.This issue affects Agrofood: from n/a before 1.4.0.	Patched by core rule	Y
CVE-2026-22467	DeepDigital — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mwtemplates DeepDigital deepdigital allows Reflected XSS.This issue affects DeepDigital: from n/a through <= 1.0.2.	Patched by core rule	Y
CVE-2026-22465	BuddyApp — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SeventhQueen BuddyApp buddyapp allows Reflected XSS.This issue affects BuddyApp: from n/a through <= 1.9.2.	Patched by core rule	Y
CVE-2026-22455	Thebe — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in foreverpinetree Thebe thebe allows Reflected XSS.This issue affects Thebe: from n/a through <= 1.3.0.	Patched by core rule	Y
CVE-2026-22440	Thecs — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in foreverpinetree Thecs thecs allows Reflected XSS.This issue affects Thecs: from n/a through <= 1.4.7.	Patched by core rule	Y
CVE-2026-22438	TheBi — Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in foreverpinetree	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		TheBi thebi allows Reflected XSS.This issue affects TheBi: from n/a through <= 1.0.5.		
CVE-2025-69343	Theater for WordPress — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeroen Schmit Theater for WordPress theatre allows Stored XSS.This issue affects Theater for WordPress: from n/a through <= 0.19.	Patched by core rule	Y
CVE-2026-3034	The OoohBoi Steroids for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the _ob_spac...	Vulnerability via the _ob_spacerat_link, _ob_bbad_link, and _ob_teleporter_link URL parameters due to insufficient input sanitization or output escaping. Affects versions up to and including 2.1.24..	Patched by core rule	Y
CVE-2026-2365	The Fluent Forms Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `fluentform_step_form_...	Vulnerability via the `fluentform_step_form_save_data` AJAX action due to insufficient input sanitization or output escaping. Affects versions up to and including 6.1.17..	Patched by core rule	Y
CVE-2019-25502	Simple Job Script contains a cross-site scripting vulnerability that allows unauthenticated attackers to inject malic...	Attackers can craft requests with SVG payload injection to execute arbitrary JavaScript in victim browsers and steal session cookies or perform unauthorized actions.	Patched by core rule	Y
CVE-2026-2355	The My Calendar — Accessible Event Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ...	Vulnerability via the `template` attribute of the `[my_calendar_upcoming]` shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 3.7.3..	Patched by core rule	Y
CVE-2026-1706	The All-in-One Video Gallery plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'vi' parame...	Vulnerability via the 'vi' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 4.7.1.	Patched by core rule	Y
CVE-2026-1236	The Envira Gallery for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'justified...	Vulnerability via the 'justified_gallery_theme' parameter due to insufficient input sanitization or output escaping. Affects versions up to and including 1.12.3.	Patched by core rule	Y
CVE-2026-28772	A Reflected Cross-Site Scripting (XSS) vulnerability in the /IDC_Logging/index.cgi endpoint of International Datacast...	A Reflected Cross-Site Scripting (XSS) vulnerability in the /IDC_Logging/index.cgi endpoint of International Datacasting Corporation (IDC) SFX Series SuperFlex SatelliteReceiver Web Management Interface version 101 allows a remote attacker to execute arbitrary web scripts or HTML. The vulnerability is triggered by sending a crafted payload through the `submitType` parameter, which is reflected directly into the DOM without proper escaping.	Patched by core rule	Y
CVE-2026-28771	A Reflected Cross-Site Scripting (XSS) vulnerability exists in the /index.cgi endpoint of International Datacasting C...	A Reflected Cross-Site Scripting (XSS) vulnerability exists in the /index.cgi endpoint of International Datacasting Corporation (IDC) SFX Series SuperFlex Satellite Receiver	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Web Management Interface version 101. The application fails to adequately sanitize user-supplied input provided via the `cat` parameter before reflecting it in the HTTP response, allowing a remote attacker to execute arbitrary HTML or JavaScript in the victim's browser context.		
CVE-2026-3242	In Concrete CMS below version 9.4.8, a rogue administrator can add stored XSS via the Switch Language block.	In Concrete CMS below version 9.4.8, a rogue administrator can add stored XSS via the Switch Language block. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks M3dium for reporting.	Patched by core rule	Y
CVE-2026-3241	In Concrete CMS below version 9.4.8, a stored cross-site scripting (XSS) vulnerability exists in the "Legacy Form" bl...	The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks M3dium for reporting.	Patched by core rule	Y
CVE-2026-3240	In Concrete CMS below version 9.4.8, a user with permission to edit a page with element Legacy form can perform a sto...	In Concrete CMS below version 9.4.8, a user with permission to edit a page with element Legacy form can perform a stored XSS attack towards high-privilege accounts via the Question field. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Thanks minhnn42, namdi and quanlna2 from VCSLab-Viettel Cyber Security for reporting.	Patched by core rule	Y
CVE-2026-3244	In Concrete CMS below version 9.4.8, A stored cross-site scripting (XSS) vulnerability exists in the search block whe...	This allows authenticated, rogue administrators to inject malicious JavaScript through page names that executes when users search for and view those pages in search results. The Concrete CMS security team gave this vulnerability a CVSS v.4.0 score of 4.8 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N. Thanks zolpak for reporting	Patched by core rule	Y
CVE-2026-2292	The Morkva UA Shipping plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all ve...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.7.9.	Patched by core rule	Y
CVE-2026-2289	The Taskbuilder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions ...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 5.0.3.	Patched by core rule	Y
CVE-2026-1945	The WPBookit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpb_user_name' and 'wpb_user_...	Vulnerability via the 'wpb_user_name' and 'wpb_user_email' parameters due to insufficient input sanitization or output escaping. Affects versions up to and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		including 1.0.8.		
CVE-2026-24415	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager v2.9.8 and earlier contains Reflected XSS vulnerabilities in invoice/order/contract modification modals. The application fails to properly sanitize user-supplied input from the righe GET parameter before reflecting it in HTML output.The $_GET['righe'] parameter is directly echoed into the HTML value attribute without any sanitization using htmlspecialchars() or equivalent functions. This allows an attacker to break out of the attribute context and inject arbitrary HTML/JavaScript.	Patched by core rule	Y
CVE-2026-21866	Dify is an open-source LLM app development platform.	Prior to 1.11.2, Dify is vulnerable to a stored XSS issue when rendering Mermaid diagrams within chats. This occurs because Dify's default Mermaid configuration uses securityLevel: loose, which allows potentially unsafe content to execute. This vulnerability is fixed in 1.11.2.	Patched by core rule	Y
CVE-2026-2568	The WP Zendesk for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms plugin for WordPress is vulnerable ...	Vulnerability via form submission data due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.5.	Patched by core rule	Y
CVE-2026-3455	Versions of the package mailparser before 3.9.3 are vulnerable to Cross-site Scripting (XSS) via the textToHtml() fun...	An attacker can execute arbitrary scripts in victim browsers by adding extra quote " to the URL with embedded malicious JavaScript code.	Patched by core rule	Y
CVE-2026-2583	The Blocksy theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `blocksy_meta` metadata fields i...	This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-52470	Chamilo is a learning management system.	Prior to version 1.11.30, a stored cross-site scripting (XSS) vulnerability exists in the session_category_add.php script. The vulnerability is caused by improper sanitization of the Category Name field, allowing privileged users to inject persistent JavaScript payloads. The injected script is later executed when accessing add_many_sessions_to_category.php, potentially compromising administrative sessions. This issue has been patched in version 1.11.30.	Patched by core rule	Y
CVE-2025-52468	Chamilo is a learning management system.	Prior to version 1.11.30, an input validation vulnerability exists when importing user data from CSV files. This flaw occurs due to insufficient sanitization of user data, specifically in the "Last Name", "First Name", and "Username" fields. It allows attackers to inject a stored	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross-site scripting (XSS) payload that is triggered when the user profile is viewed, potentially leading to malicious script execution in the context of the authenticated use. This issue has been patched in version 1.		
CVE-2025-52482	Chamilo is a learning management system.	Prior to version 1.11.30, a Stored XSS vulnerability exists in the glossary function, enabling all users with the Teachers role to inject JavaScript malicious code against the administrator. This issue has been patched in version 1.11.30.	Patched by core rule	Y
CVE-2025-50186	Chamilo is a learning management system.	Prior to version 1.11.30, a stored cross-site scripting (XSS) vulnerability exists due to insufficient sanitization of CSV filenames. An attacker can upload a maliciously named CSV file (e.g., <img src=q onerror=prompt(8)>.csv) that leads to JavaScript execution when viewed by administrators or users with access to import logs or file views. This issue has been patched in version 1.11.30.	Patched by core rule	Y
CVE-2026-3412	itsourcecode University Management System — Cross-Site Scripting	This affects an unknown part of the file /att_single_view.php. The manipulation of the argument dt results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-3403	PHPGurukul Student Record Management System — Cross-Site Scripting	This issue affects some unknown processing of the file /edit-subject.php. Performing a manipulation of the argument Subject 1 results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-3402	PHPGurukul Student Record Management System up to — Cross-Site Scripting	Such manipulation of the argument Course Short Name leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-28338	PMD is an extensible multilanguage static code analyzer.	Prior to version 7.22.0, PMD's `vbhtml` and `yahtml` report formats insert rule violation messages into HTML output without escaping. When PMD analyzes untrusted source code containing crafted string literals, the generated HTML report contains executable JavaScript that runs when opened in a browser. Practical impact is limited because `vbhtml` and `yahtml` are legacy formats rarely used in practice. The default `html` format is properly escaped and not affected. Version 7.22.	Patched by core rule	Y
CVE-2026-26997	ClipBucket v5 is an open source video sharing platform.	Prior to version 5.5.3 #59, a normal authenticated user can store the XSS payload. The payload is triggered by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		administrator. Version 5.5.3 #59 fixes the issue.		
CVE-2026-26862	CleverTap Web SDK version 1.15.2 and earlier is vulnerable to DOM-based Cross-Site Scripting (XSS) via window.postMes...	The origin validation in src/modules/visualBuilder/pageBuilder.js (lines 56-60) uses the includes() method to verify the originUrl contains "dashboard.clevertap.com", which can be bypassed by an attacker using a crafted subdomain	Patched by core rule	Y
CVE-2026-26861	CleverTap Web SDK version 1.15.2 and earlier is vulnerable to Cross-Site Scripting (XSS) via window.postMessage.	The handleCustomHtmlPreviewPostMessageEvent function in src/util/campaignRender/nativeDisplay.js performs insufficient origin validation using the includes() method, which can be bypassed by an attacker using a subdomain	Patched by core rule	Y
CVE-2025-69437	PublicCMS v5.202506.d and earlier is vulnerable to stored XSS.	Uploaded PDFs can contain JavaScript payloads and bypass PDF security checks in the backend CmsFileUtils.java. If a user uploads a PDF file containing a malicious payload to the system and views it, the embedded JavaScript payload can be triggered, resulting in issues such as credential theft, arbitrary API execution, and other security concerns.	Patched by core rule	Y
CVE-2025-14142	The Electric Enquiries plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button' parameter o...	Vulnerability via the 'button' parameter of the electric-enquiry shortcode due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1.	Patched by core rule	Y
CVE-2026-2383	The Simple Download Monitor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom field in all...	Vulnerability via custom field due to insufficient input sanitization or output escaping. Affects versions up to and including 4.0.5.	Patched by core rule	Y
CVE-2026-2362	The WP Accessibility plugin for WordPress is vulnerable to Stored DOM-Based Cross-Site Scripting via the 'alt' attrib...	Vulnerability via the 'alt' attribute of images processed by the "Long Description UI" feature due to insufficient input sanitization or output escaping. Affects versions up to and including 2.3.1..	Patched by core rule	Y
CVE-2026-3302	SourceCodester Doctor Appointment System — Cross-Site Scripting	Executing a manipulation of the argument Email can lead to cross site scripting. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2025-14149	The Xpro Addons ,Äî 140+ Widgets for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via ...	Vulnerability via the plugin's Image Scroller widget box link attribute due to insufficient input sanitization or output escaping. Affects versions up to and including 1.4.24.	Patched by core rule	Y
CVE-2025-14040	The Automotive Car Dealership Business WordPress Theme for WordPress is vulnerable to Stored Cross-Site Scripting via...	This is due to insufficient input sanitization and output escaping on user-supplied attributes in the 'action_text', 'action_button_text', 'action_link', and 'action_class' custom fields. This makes it possible for authenticated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2026-28274	Initiative is a self-hosted project management platform.	Versions of the application prior to 0.32.4 are vulnerable to Stored Cross-Site Scripting (XSS) in the document upload functionality. Any user with upload permissions within the "Initiatives" section can upload a malicious `.html` or `.htm` file as a document. Because the uploaded HTML file is served under the application's origin without proper sandboxing, the embedded JavaScript executes in the context of the application.	Patched by core rule	Y
CVE-2026-28083	Flatsome — Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UX-themes Flatsome flatsome allows Stored XSS.This issue affects Flatsome: from n/a through <= 3.20.1.	Patched by core rule	Y
CVE-2026-27963	Audiobookshelf is a self-hosted audiobook and podcast server.	A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.32.0 of the Audiobookshelf web application that allows arbitrary JavaScript execution through malicious library metadata. Attackers with library modification privileges can execute code in victim users' browsers, potentially leading to session hijacking and data exfiltration. Version 2.32.0 contains a patch for the issue.	Patched by core rule	Y
CVE-2026-2506	The EM Cost Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and inclu...	This is due to the plugin storing attacker-controlled 'customer_name' data and rendering it in the admin customer list without output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator views the EMCC Customers page.	Patched by core rule	Y
CVE-2026-2499	The Custom Logo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions ...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 2.2.	Patched by core rule	Y
CVE-2026-2498	The WP Social Meta plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versio...	Vulnerability via admin settings due to insufficient input sanitization or output escaping. Affects versions up to and including 1.0.1.	Patched by core rule	Y
CVE-2026-2489	The TP2WP Importer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Watched domains' textar...	Vulnerability via the 'Watched domains' textarea on the attachment importer settings page due to insufficient input sanitization or output escaping. Affects versions up to and including 1.1..	Patched by core rule	Y
CVE-2026-2029	The Livemesh Addons for Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting	Vulnerability via the `[labb_pricing_item]` shortcode's `title` and `value` attributes due to insufficient	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	via the `[la...	input sanitization or output escaping. Affects versions up to and including 3.9.2.		
CVE-2026-27616	Vikunja is an open-source self-hosted task management platform.	Prior to version 2.0.0, the application allows users to upload SVG files as task attachments. SVG is an XML-based format that supports JavaScript execution through elements such as <script> tags or event handlers like onload. The application does not sanitize SVG content before storing it. When the uploaded SVG file is accessed via its direct URL, it is rendered inline in the browser under the application's origin.	Patched by core rule	Y
CVE-2026-27116	Vikunja is an open-source self-hosted task management platform.	Prior to version 2.0.0, a reflected HTML injection vulnerability exists in the Projects module where the `filter` URL parameter is rendered into the DOM without output encoding when the user clicks "Filter." While `<script>` and `<iframe>` are blocked, `<svg>`, `<a>`, and formatting tags (`<h1>`, `<b>`, `<u>`) render without restriction — enabling SVG-based phishing buttons, external redirect links, and content spoofing within the trusted application origin. Version 2.0.0 fixes this issue.	Patched by core rule	Y
CVE-2026-25736	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific...	Versions prior to 35.8.3, 38.5.4, and 39.3.1 have a stored Cross-Site Scripting (XSS) vulnerability in the Custom RSE Attribute of the WebUI where attacker-controlled input is persisted by the backend and later rendered in the WebUI without proper output encoding. This allows arbitrary JavaScript execution in the context of the WebUI for users who view affected pages, potentially enabling session token theft or unauthorized actions. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	Patched by core rule	Y
CVE-2026-25735	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific...	Versions prior to 35.8.3, 38.5.4, and 39.3.1 have a stored Cross-Site Scripting (XSS) vulnerability in the Identity Name of the WebUI where attacker-controlled input is persisted by the backend and later rendered in the WebUI without proper output encoding. This allows arbitrary JavaScript execution in the context of the WebUI for users who view affected pages, potentially enabling session token theft or unauthorized actions. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	Patched by core rule	Y
CVE-2026-25734	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific...	Versions prior to 35.8.3, 38.5.4, and 39.3.1 have a stored Cross-Site Scripting (XSS) vulnerability in the RSE metadata of the WebUI where attacker-controlled input is persisted by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the backend and later rendered in the WebUI without proper output encoding. This allows arbitrary JavaScript execution in the context of the WebUI for users who view affected pages, potentially enabling session token theft or unauthorized actions. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.		
CVE-2026-25733	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific...	Versions prior to 35.8.3, 38.5.4, and 39.3.1 have a stored Cross-Site Scripting (XSS) vulnerability in the Custom Rules function of the WebUI where attacker-controlled input is persisted by the backend and later rendered in the WebUI without proper output encoding. This allows arbitrary JavaScript execution in the context of the WebUI for users who view affected pages, potentially enabling session token theft or unauthorized actions. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	Patched by core rule	Y
CVE-2026-25136	Rucio is a software framework that provides functionality to organize, manage, and access large volumes of scientific...	A reflected Cross-site Scripting vulnerability was located in versions prior to 35.8.3, 38.5.4, and 39.3.1 in the rendering of the ExceptionMessage of the WebUI 500 error which could allow attackers to steal login session tokens of users who navigate to a specially crafted URL. Versions 35.8.3, 38.5.4, and 39.3.1 fix the issue.	Patched by core rule	Y
CVE-2026-25743	OpenEMR is a free and open source electronic health records and medical practice management application.	Prior to version 8.0.0, users with the "Forms administration" role can fill questionnaires ("forms") in patient encounters. The answers to the forms are displayed on the encounter page and in the visit history for the users with the same role.	Patched by core rule	Y

Prompt Injection Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-30741	OpenClaw Agent Platform — RCE via Request-Side Prompt Injection.	A remote code execution (RCE) vulnerability in OpenClaw Agent Platform v2026.2.6 allows attackers to execute arbitrary code via a Request-Side prompt injection attack.	Patched by core rule	Y

Monthly Zero-Day Vulnerability Coverage Bulletin March 2026

INDUSFACE™

Indusface is a leading application security SaaS company, securing over 6,500 customers across 95 countries with its award-winning platform. Backed by leading institutional investors, Indusface is a category leader in cloud WAAP, with repeated recognition from top analysts and industry platforms including Gartner, Forrester, GigaOm, and G2.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 4 consecutive years

A Customers' Choice from 2022 to 2024 Gartner® Peer Insights™

CONTACT US - +91 265 6133021 | +1 866 537 8234