INDUSFACE™

MONTHLY BULLETIN · MAY 2026

Zero-Day Vulnerability Coverage Report

Comprehensive AppTrana and Indusface WAS protection coverage across all newly disclosed zero-day vulnerabilities for May 2026.

271	100%	99%
TOTAL ZERO-DAYS	CORE RULE COVERAGE	WAS SCANNER COVERAGE

EXECUTIVE SUMMARY

May 2026 - Vulnerability Coverage Overview

AppTrana protected against 271 newly disclosed zero-day vulnerabilities across eight attack categories. The Indusface WAS scanner and AppTrana's core rules delivered 99% and 100% coverage respectively, with no custom rule patches required.

VULNERABILITY BREAKDOWN

VULNERABILITY CATEGORY	COUNT
Command Injection	44
SQL Injection	50
SSRF	31
Cross-Site Scripting	98
Code Injection	29
Path Traversal	8
Malicious File Upload	7
Design and Config Vulnerabilities	4

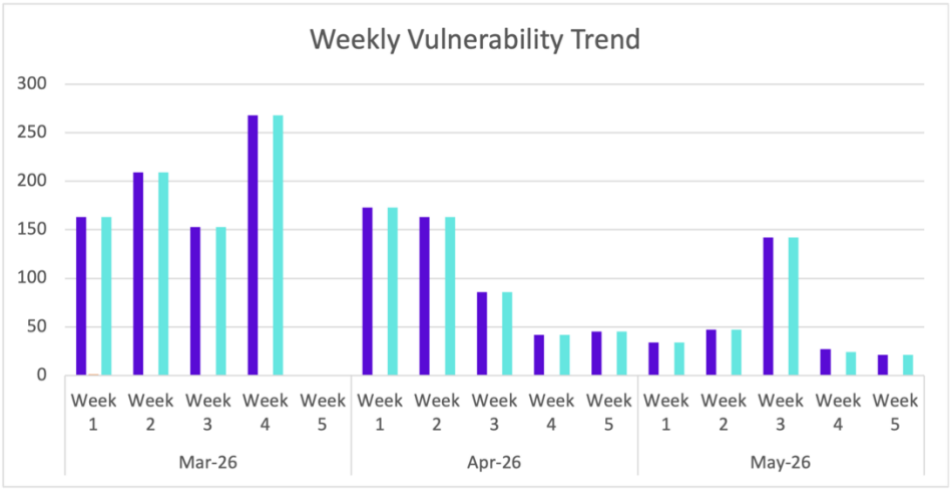
COVERAGE BY THE NUMBERS

COVERAGE METRIC	COUNT
Zero-day vulnerabilities protected through core rules	271
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	268

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

VULNERABILITY TREND

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



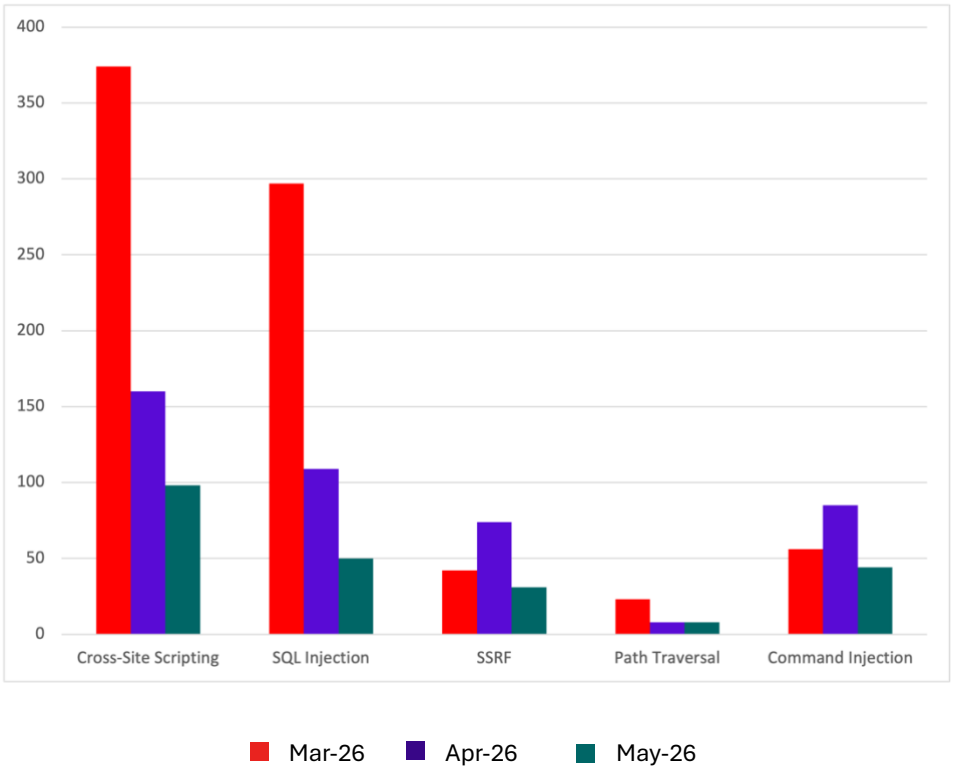
100%

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

99%

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

TOP FIVE VULNERABILITY CATEGORIES



VULNERABILITY DETAILS

Command Injection Vulnerabilities

Command injection vulnerabilities allow attackers to execute arbitrary OS commands by injecting shell metacharacters into unsanitized parameters. All 44 command injection CVEs identified in May 2026 are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-45585	Windows Security Feature Bypass – "YellowKey"	Microsoft is aware of a security feature bypass vulnerability in Windows publicly referred to as "YellowKey". The proof of concept for this vulnerability has been made public violating coordinated vulnerability best practices. We are issuing this CVE to provide mitigation guidance that can be implemented to protect against this vulnerability until the security update is made available. Mitigation FAQs Should I leverage the temporary mitigation? Microsoft recommends that you consider implementing these mitigations if you are concerned your devices and data are at risk of being compromised or stolen. For example, if your organization,Äôs employees take their work devices home or on business travel. What impact to service availability/management could be caused by implementing the mitigations? Implementing these mitigations will not impact service availability or management operations. Do customers need to revert the changes made to mitigate the vulnerability once the security update to protect against this vulnerability is available? No. The security update will maintain the mitigation's	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		behavior once the security update is installed. I am using TPM+PIN, am I at risk of this vulnerability being exploited No, if you are using TPM+PIN the vulnerability is not exploitable.		
CVE-2026-25244	WebdriverIO Test Automation Framework Vulnerability	WebdriverIO is a test automation framework for unit, e2e and component testing using WebDriver, WebDriver BiDi and Appium. Versions below 9.24.0 contain a command injection vulnerability leading to remote code execution (RCE) in test orchestration. Git permits branch names containing shell metacharacters, and getGitMetadataForAISelection() interpolates these names directly into execSync() calls without sanitization. An attacker can exploit this by supplying a malicious repository (via testOrchestrationOptions.runSmartSelection.source, or the current directory if unset) whose branch name carries a payload, causing the shell to execute arbitrary code. This enables remote code execution on CI/CD servers and developer machines, leading to credential and secret disclosure, source code and SSH key exfiltration, system compromise, and supply chain attacks via tampered build artifacts. The issue has been fixed in version 9.24.0.	Patched by core rule	Y
CVE-2026-8767	Vercel AI (≤3.0.97) Vulnerability	A vulnerability has been found in vercel ai up to 3.0.97. Impacted is the function run of the file .github/workflows/prettier-on-automerge.yml of the component PR Branch Name Interpolation. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to os command injection. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitability is considered difficult. 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.		
CVE-2026-45035	Tabby (Terminus) Terminal Emulator Vulnerability	Tabby (formerly Terminus) is a highly configurable terminal emulator. Prior to 1.0.233, Tabby registers itself as the handler for the tabby:// URL scheme on all platforms. The URL scheme handler supports a run command that directly executes OS commands with no user confirmation, sanitization, or sandboxing. An attacker can craft a malicious link (tabby://run?command=...) and deliver it via a website, email, chat message, or any other medium. When a victim clicks the link, the OS launches Tabby which immediately spawns the specified command as a child process with the user's full privileges. This is a zero-click-after-link-visit RCE vulnerability. This vulnerability is fixed in 1.0.233.	Patched by core rule	Y
CVE-2026-41315	mdserver-web Linux Panel Vulnerability	mdserver-web is a simple Linux panel. From 0.18.0 to 0.18.4, mdserver-web has a front-end unauthorized remote command execution vulnerability. Due to the lack of authentication on the /modify_crond and /start_task interfaces, it is possible to modify the default built-in scheduled tasks and start them, achieving RCE.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-42589	Gotenberg PDF API Vulnerability	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.31.0, Gotenberg's /forms/pdfengines/metadata/write HTTP endpoint accepts a JSON metadata object and passes its keys directly to ExifTool via the go-exiftool library. No validation is performed on key characters. A \n embedded in a JSON key splits the ExifTool stdin stream into a new argument line, allowing an attacker to inject arbitrary ExifTool flags ,Äî including -if, which evaluates Perl expressions. This achieves unauthenticated OS command execution in a single HTTP request. The response is HTTP 200 with a valid PDF, making the attack transparent to basic monitoring. This vulnerability is fixed in 8.31.0.	Patched by core rule	Y
CVE-2026-44194	OPNsense Firewall & Routing Platform Vulnerability	OPNsense is a FreeBSD based firewall and routing platform. Prior to 26.1.8, an authenticated Remote Code Execution (RCE) vulnerability in the OPNsense core allows a user with user-management privileges to execute arbitrary system commands as root. An attacker can bypass input validation by formatting their malicious payload as a compliant email address, allowing shell commands to reach the underlying operating system. The flaw exists in the local user synchronization flow, within core/src/opnsense/scripts/auth/sync_user.php. This vulnerability is fixed in 26.1.8.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-31226	TinyZero HDFS Utilities Command Injection	The TinyZero project thru commit 6652a63c57fa7e5ccde3fc9c598c7176ff15b839 (2025-58-24) contains a critical command injection vulnerability (CWE-78) in its HDFS file operation utilities. The vulnerability arises from the unsafe construction and execution of shell commands via os.system() without proper input sanitization or escaping. User-controlled input (such as file paths) is directly interpolated into shell command strings using f-strings within the _copy() function. An attacker can inject arbitrary OS commands by supplying a specially crafted path parameter through the Hydra configuration framework. This leads to remote code execution with the privileges of the user running the TinyZero training process.	Patched by core rule	Y
CVE-2026-36983	D-Link DCS-932L v2.18.01 Command Injection	D-Link DCS-932L v2.18.01 is vulnerable to Command Injection in the function sub_42EF14 of the file /bin/alphapd. The manipulation of the argument LightSensorControl leads to command injection.	Patched by core rule	Y
CVE-2026-31246	GPT-Pilot Executor.run() Command Injection	GPT-Pilot thru commit 0819827ce20346ef5f25b3fe29293cb448840565 (2025-09-03) contains a command injection vulnerability (CWE-78) in the Executor.run() method. During project execution, when the system prompts the user to confirm or modify a command to be run, it accepts free-text input without proper validation. The user-supplied input is directly	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		passed to asyncio.create_subprocess_shell() for execution. This allows an attacker to replace the intended command with arbitrary shell commands, leading to remote code execution with the privileges of the GPT-Pilot process.		
CVE-2026-8273	D-Link DNS-320 2.06B01 Weakness	A weakness has been identified in D-Link DNS-320 2.06B01. This impacts the function cgi_set_host/cgi_set_ntp/cgi_fan_control/cgi_merge_user of the file /cgi-bin/system_mgr.cgi. This manipulation causes os command injection. It is possible to initiate the attack remotely.	Patched by core rule	Y
CVE-2026-8272	D-Link DNS-320 2.06B01 Security Flaw	A security flaw has been discovered in D-Link DNS-320 2.06B01. This affects the function delete/rename/copy/move/chmod/chown of the file /cgi-bin/webfile_mgr.cgi. The manipulation results in os command 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-2026-8271	D-Link DNS-320 2.06B01 Vulnerability	A vulnerability was identified in D-Link DNS-320 2.06B01. The impacted element is the function cgi_speed/cgi_dhcpd_lease/cgi_ddns/cgi_set_ip/cgi_upnp_del/cgi_dhcpd/cgi_upnp_add/cgi_upnp_edit of the file /cgi-bin/network_mgr.cgi. The manipulation leads to os command injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-8265	Tenda AC6 15.03.06.23 Security Vulnerability	A security vulnerability has been detected in Tenda AC6 15.03.06.23. Affected by this issue is the function get_log_file of the file /goform/getLogFile of the component httpd. The manipulation of the argument wans.flag leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-8264	Tenda AC6 15.03.06.23 Weakness	A weakness has been identified in Tenda AC6 15.03.06.23. Affected by this vulnerability is the function formWifiApScan of the file /goform/WifiApScan of the component httpd. Executing a manipulation of the argument wl2g.public.country/wl5g.public.country can lead to os command 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-2026-8263	Tenda AC6 15.03.06.49_multi_TDE01 Security Flaw	A security flaw has been discovered in Tenda AC6 15.03.06.49_multi_TDE01. Affected is the function fromSetWirelessRepeat of the file /goform/WifiExtraSet of the component httpd. Performing a manipulation of the argument mac/ssid results in os command injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-8259	Tenda AC6 2.0/15.03.06.23 Vulnerability	A vulnerability has been found in Tenda AC6 2.0/15.03.06.23. The affected element is an unknown function of the file /goform/telnet of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component httpd. The manipulation of the argument lan.ip leads to os command injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.		
CVE-2026-8230	Wavlink NU516U1 240425 Flaw	A flaw has been found in Wavlink NU516U1 240425. The impacted element is the function sys_login1 of the file /cgi-bin/login.cgi. Executing a manipulation of the argument ipaddr can lead to os command injection. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2026-8229	Wavlink NU516U1 240425 Vulnerability	A vulnerability was detected in Wavlink NU516U1 240425. The affected element is the function WifiBasic of the file /cgi-bin/wireless.cgi. Performing a manipulation of the argument AuthMethod/EncrypType results in os command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2026-8228	Wavlink NU516U1 240425 Security Vulnerability	A security vulnerability has been detected in Wavlink NU516U1 240425. Impacted is the function advance of the file /cgi-bin/wireless.cgi. Such manipulation of the argument wlan_conf/Channel/skiplist/ieee_80211h leads to os command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		was contacted early about this disclosure.		
CVE-2026-8227	Wavlink NU516U1 240425 Weakness	A weakness has been identified in Wavlink NU516U1 240425. This issue affects the function wzdapMesh of the file /cgi-bin/adm.cgi. This manipulation causes os command injection. 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.	Patched by core rule	Y
CVE-2026-8192	Wavlink NU516U1 M16U1_V240425 Security Flaw	A security flaw has been discovered in Wavlink NU516U1 M16U1_V240425. This vulnerability affects the function wzdap of the file /cgi-bin/adm.cgi. Performing a manipulation of the argument EncrypType/wl_Pass is directly passed by the attacker/so we can control the EncrypType/wl_Pass results in os command injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2026-8191	Wavlink NU516U1 M16U1_V240425 Vulnerability	A vulnerability was identified in Wavlink NU516U1 M16U1_V240425. This affects the function wifi_region of the file /cgi-bin/adm.cgi. Such manipulation of the argument skiplist1/skiplist2 leads to os command injection. The attack can be launched remotely. The exploit is publicly available and might be used. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vendor was contacted early about this disclosure.		
CVE-2026-8190	Wavlink NU516U1 M16U1_V240425 Vulnerability	A vulnerability was determined in Wavlink NU516U1 M16U1_V240425. Affected by this issue is the function wan of the file /cgi-bin/adm.cgi. This manipulation of the argument ppp_username/ppp_passwd/rwan_ip/rwan_mask/rwan_gateway is directly passed by the attacker/so we can control the ppp_username/ppp_passwd/rwan_ip/rwan_mask/rwan_gateway causes os command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2026-8189	Wavlink NU516U1 M16U1_V240425 Vulnerability	A vulnerability was found in Wavlink NU516U1 M16U1_V240425. Affected by this vulnerability is the function wzdrepeater of the file /cgi-bin/adm.cgi. The manipulation of the argument wlan_bssid/sel_Automode/sel_EncrypTyp results in os command injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2026-8188	Wavlink NU516U1 M16U1_V240425 Vulnerability	A vulnerability has been found in Wavlink NU516U1 M16U1_V240425. Affected is the function change_wifi_password of the file /cgi-bin/adm.cgi. The manipulation of the argument wl_channel/wl_Pass/EncrypType leads to os command	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.		
CVE-2026-41497	PraisonAI Multi-Agent System Vulnerability	PraisonAI is a multi-agent teams system. Prior to version 4.6.9, the fix for PraisonAI's MCP command handling does not add a command allowlist or argument validation to parse_mcp_command(), allowing arbitrary executables like bash, python, or /bin/sh with inline code execution flags to pass through to subprocess execution. This issue has been patched in version 4.6.9.	Patched by core rule	Y
CVE-2024-51092	LibreNMS Remote Code Execution via OS Command Injection	LibreNMS before 24.10.0 allows a remote attacker to execute arbitrary code via OS command injection involving AboutController.php's index(), SettingsController.php's update(), and PollDevice.php's initRrdDirectory().	Patched by core rule	Y
CVE-2024-45257	BYOB 2.0 Payload Build Page Command Injection	A Command Injection issue in the payload build page in BYOB (Build Your Own Botnet) 2.0 allows attackers to execute arbitrary commands on the server via a crafted build parameter. This occurs in freeze in core/generators.py.	Patched by core rule	Y
CVE-2023-47268	PrusaSlicer 3MF Project File Arbitrary Code Execution	In libslic3r/GCode/PostProcessor.cpp in Prusa PrusaSlicer through 2.6.1, a crafted 3mf project file can execute arbitrary code on a host where the project is sliced and G-code exported.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45899	Nokia BMC Log Scanner OS Command Injection (Unauthenticated)	Nokia Broadcast Message Center (BMC) before 13.1 allows an unauthenticated remote attacker to do OS command injection as root via shell metacharacters in the Log Scanner Search Pattern field.	Patched by core rule	Y
CVE-2026-8112	8421bit MiniClaw Vulnerability	A vulnerability was found in 8421bit MiniClaw up to 223c16a1088e138838dcbd18cd65a37c35ac5a84. Affected is the function executeCognitivePulse of the file src/kernel.ts. Performing a manipulation results in os command injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The patch is named 028f62216dee9f64833d0f1cfda7c217067ceba8. To fix this issue, it is recommended to deploy a patch.	Patched by core rule	Y
CVE-2026-42215	GitPython Git Library Vulnerability	GitPython is a python library used to interact with Git repositories. From version 3.1.30 to before version 3.1.47, GitPython blocks dangerous Git options such as --upload-pack and --receive-pack by default, but the equivalent Python kwargs upload_pack and receive_pack bypass that check. If an application passes attacker-controlled kwargs into Repo.clone_from(), Remote.fetch(), Remote.pull(), or Remote.push(), this leads to arbitrary command execution even when	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allow_unsafe_options is left at its default value of False. This issue has been patched in version 3.1.47.		
CVE-2026-7609	TRENDnet TEW-821DAP (≤1.12B01) Flaw	A flaw has been found in TRENDnet TEW-821DAP up to 1.12B01. The impacted element is the function tools_diagnostic of the file /tmp/diagnostic of the component Firmware Udpate. This manipulation causes os command injection. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-7608	TRENDnet TEW-821DAP (≤1.12B01) Vulnerability	A vulnerability was detected in TRENDnet TEW-821DAP up to 1.12B01. The affected element is the function tools_diagnostic. The manipulation results in os command injection. The exploit is now public and may be used. The vendor explains: "That firmware version will only work on our hardware version v1.xR. We have already EOL that product 8 years ago and are no longer selling". This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-7551	HKUDS OpenHarness Remote Code Execution via /bridge Slash Command	HKUDS OpenHarness contains a remote code execution vulnerability in the /bridge slash command that allows remote senders accepted by configuration to execute arbitrary operating	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		system commands. Attackers can invoke the /bridge spawn command with attacker-controlled command text that is forwarded to the bridge session manager and executed through the shared shell subprocess helper, allowing them to spawn shell sessions as the OpenHarness process user and access local files, credentials, workspace state, and repository contents.		
CVE-2025-71284	Synway SMG Gateway RADIUS Config OS Command Injection	Synway SMG Gateway Management Software contains an OS command injection vulnerability in the RADIUS configuration endpoint at /en/9-2radius.php where the radius_address POST parameter is split and interpolated directly into a sed command without sanitization. An unauthenticated remote attacker can inject arbitrary shell commands by submitting a POST request with crafted radius_address, radius_address2, shared_secret2, source_ip, timeout, or retry parameters along with save=1 and enable_radius=1 to achieve remote code execution. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-07-11 (UTC).	Patched by core rule	Y
CVE-2026-7246	Pallets Click (≤8.3.2) click.edit() Command Injection	Pallets Click, versions 8.3.2 and below, contain a command injection vulnerability in the click.edit() function, allowing attackers to pass arbitrary OS commands from an unprivileged account.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-26015	DocsGPT Documentation Chat Vulnerability	DocsGPT is a GPT-powered chat for documentation. From version 0.15.0 to before version 0.16.0, an attacker accessing both the official DocsGPT website or any local and public deployment, can craft a malicious payload bypassing the "MCP test" behavior to achieve arbitrary remote code execution (RCE). This issue has been patched in version 0.16.0.	Patched by core rule	Y
CVE-2026-31255	Tenda AC18 V15.03.05.05_multi Command Injection	A command injection vulnerability exists in Tenda AC18 V15.03.05.05_multi. The vulnerability is located in the /goform/SetSambaCfg interface, where improper handling of the guestuser parameter allows attackers to execute arbitrary system commands.	Patched by core rule	Y
CVE-2026-7119	Tenda HG3 2.0 Vulnerability	A vulnerability was detected in Tenda HG3 2.0. The impacted element is an unknown function of the file /boaform/formCountrystr. The manipulation of the argument countrystr results in os command injection. The attack may be performed from remote. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-7096	Tenda HG3 2.0 300003070 Security Flaw	A security flaw has been discovered in Tenda HG3 2.0 300003070. This vulnerability affects the function formgponConf of the file /boaform/admin/formgponConf. The manipulation of the argument fmgpon_loid results in os command injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-29014	MetInfo CMS Remote Code Execution	MetInfo CMS contains a remote code execution vulnerability in its template processing engine. Authenticated attackers can inject PHP code through the CMS template editor interface, which is then executed on the server when the affected page is rendered. Successful exploitation grants the attacker full control over the web server process, enabling file system access, credential theft, and lateral movement. This vulnerability is covered by AppTrana's core injection-detection rules that block server-side code execution payloads in HTTP requests.	Patched by core rule	Y
CVE-2026-8711	NGINX Remote Code Execution	A remote code execution vulnerability has been identified in NGINX affecting specific versions of the web server. The flaw arises from improper handling of crafted HTTP requests that can trigger memory corruption or module-level command injection in vulnerable NGINX configurations. Exploitation allows an unauthenticated remote attacker to execute arbitrary code with the privileges of the NGINX worker process. Mitigation is applied at the infrastructure level, where network-layer controls and server hardening policies prevent exploitation before malicious traffic reaches the application.	Patched by core rule	NA

VULNERABILITY DETAILS

Path Traversal Vulnerabilities

Path traversal vulnerabilities allow attackers to access or overwrite files outside the intended directory by exploiting insufficient validation of user-supplied file paths. All 8 path traversal CVEs in May 2026 are covered by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2018-25374	MedDream PACS Server Premium 6.7.1.1 Directory Traversal (Unauthenticated)	Softneta MedDream PACS Server Premium 6.7.1.1 contains a directory traversal vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating the path parameter. Attackers can send requests to nocache.php with encoded backslash sequences to traverse directories and access sensitive files including system configuration and password files.	Patched by core rule	Y
CVE-2026-34926	Trend Micro Apex One Server Directory Traversal – Malicious Code Injection	A directory traversal vulnerability in the Apex One (on-premise) server could allow a pre-authenticated local attacker to modify a key table on the server to inject malicious code to deploy to agents on affected installations. This vulnerability is only exploitable on the on-premise version of Apex One and a potential attacker must have access to the Apex One Server and already obtained administrative credentials to the server via some other method to exploit this vulnerability.	Patched by core rule	Y
CVE-2021-47978	ProcessMaker 3.5.4 Local File Inclusion via Path Traversal	ProcessMaker 3.5.4 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting improper path traversal validation.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Attackers can send requests with directory traversal sequences to access sensitive system files like /etc/passwd without authentication.		
CVE-2021-47942	HACS (< 1.10.0) Path Traversal via /hacsfiles/ Endpoint	Home Assistant Community Store (HACS) prior to 1.10.0 contains a path traversal vulnerability that allows unauthenticated attackers to read sensitive files by traversing directories via the /hacsfiles/ endpoint. Attackers can retrieve the .storage/auth file containing user credentials and refresh tokens, then craft valid JWT tokens to gain administrative access to Home Assistant instances.	Patched by core rule	Y
CVE-2026-31156	OpenPLC v3 glue_generator.cpp Path Injection	A path injection vulnerability exists in OpenPLC v3 (2c82b0e79c53f8c1f1458eee15fec173400d6e1a) as the binary program compiled from glue_generator.cpp does not perform any validation on the file path parameters passed via the command line. The user-controlled input parameters are directly passed to the underlying file operation functions (fopen/ifstream/ofstream) for file reading and writing. An attacker can exploit this vulnerability by constructing a malicious path to read arbitrary readable files.	Patched by core rule	Y
CVE-2026-42608	Grav File-Based Web Platform Vulnerability	Grav is a file-based Web platform. Prior to 2.0.0-beta.2, there is a Path Traversal vulnerability within the FormFlash core component. By manipulating the session_id (passed as __form-flash-id in POST requests), an unauthenticated attacker can traverse the filesystem	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to create arbitrary directories and write an index.yaml file containing attacker-controlled data. This vulnerability can lead to unauthorized modification of application behavior, potential data integrity issues, and service disruption in production environments. This vulnerability is fixed in 2.0.0-beta.2.		
CVE-2026-40075	OpenMRS Core Electronic Medical Record Platform Vulnerability	OpenMRS Core is an open source electronic medical record system platform. In versions 2.7.8 and earlier and versions 2.8.0 through 2.8.5, the `/openmrs/moduleResources/{moduleid}` endpoint is vulnerable to a path traversal attack. The ModuleResourcesServlet constructs a filesystem path from user-controlled input without performing path boundary validation ,Äî the getFile() method concatenates the user-supplied path into an absolute filesystem path without calling normalize() or checking that the result stays within the allowed module resources directory. Because this endpoint serves static resources required for rendering the login page, it is not protected by authentication filters, allowing unauthenticated exploitation. An attacker can traverse directories and read arbitrary files from the server filesystem, including /etc/passwd and application configuration files containing database credentials. Successful exploitation requires the target deployment to run on Apache Tomcat versions	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		prior to 8.5.31, where the ..; path parameter bypass is not mitigated by the container. Deployments on Tomcat 8.5.31 or later and Tomcat 9.0.10 or later are protected at the container level, though the underlying code defect remains. This issue has been fixed in versions after 2.7.8 (within the 2.7.x branch) and in version 2.8.6 and later.		
CVE-2018-25311	VideoFlow DVP 2.10 Authenticated Directory Traversal	VideoFlow Digital Video Protection DVP 2.10 contains an authenticated directory traversal vulnerability that allows attackers with valid credentials to disclose arbitrary files by injecting path traversal sequences in the ID parameter. Attackers can submit requests to downloadsys.pl, download_xml.pl, download.pl, downloadmib.pl, or downloadFile.pl with directory traversal payloads to read sensitive system files like /etc/passwd.	Patched by core rule	Y

VULNERABILITY DETAILS

SQL Injection Vulnerabilities

SQL injection vulnerabilities exploit insufficient input sanitization to manipulate database queries, enabling data exfiltration, authentication bypass, and in some cases remote code execution. All 50 SQL injection CVEs in May 2026 are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2018-25381	Joomla Responsive Portfolio 1.6.1 Authenticated SQL Injection	Joomla Responsive Portfolio 1.6.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL commands through multiple filter parameters. Attackers can inject malicious SQL code via the filter_type_id, filter_pid_id, and filter_search parameters in POST requests to extract sensitive database information including credentials and server details.	Patched by core rule	Y
CVE-2018-25380	Joomla eXtroForms 2.1.5 Authenticated SQL Injection	Joomla Component eXtroForms 2.1.5 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL commands through the filter_type_id, filter_pid_id, and filter_search parameters. Attackers can submit POST requests to the extroformfield view with malicious SQL payloads to extract sensitive database information and server data.	Patched by core rule	Y
CVE-2018-25379	Collectric CMU 1.0 Unauthenticated Blind SQL Injection	Collectric CMU 1.0 contains a boolean-based blind SQL injection vulnerability in the lang parameter that allows unauthenticated attackers to manipulate database queries during authentication. Attackers can inject SQL code through the lang parameter in login requests to extract sensitive information from the database using time-based blind techniques.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2018-25372	MedDream PACS Server Premium 6.7.1.1 Unauthenticated SQL Injection	MedDream PACS Server Premium 6.7.1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the email parameter. Attackers can submit crafted POST requests to the userSignup.php endpoint with SQL payloads in the email field to extract sensitive database information from the backend MySQL database.	Patched by core rule	Y
CVE-2018-25371	mooSocial Store Plugin 2.6 Unauthenticated Blind SQL Injection	mooSocial Store Plugin 2.6 contains a blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries through the product parameter in URL rewrite functionality. Attackers can inject SQL code using boolean-based blind, time-based blind, or stacked query techniques in the product URI parameter to extract sensitive database information.	Patched by core rule	Y
CVE-2018-25364	Twitter-Clone 1 Unauthenticated SQL Injection (name parameter)	Twitter-Clone 1 contains a SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the name parameter. Attackers can submit crafted payloads to the search.php endpoint to extract database information including usernames, credentials, and system data using error-based and union-based SQL injection techniques.	Patched by core rule	Y
CVE-2018-25362	Twitter-Clone 1 SQL Injection in follow.php	Twitter-Clone 1 contains a SQL injection vulnerability in follow.php that allows attackers to manipulate database queries by injecting SQL code through the userid parameter. Attackers can submit union-based or time-based blind SQL injection	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		payloads to extract sensitive database information including usernames, passwords, and database credentials.		
CVE-2018-25352	WordPress Ultimate Form Builder Lite (≤1.3.7) Authenticated SQL Injection	WordPress Ultimate Form Builder Lite plugin version 1.3.7 and below contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the entry_id POST parameter. Attackers can send POST requests to the admin-ajax.php endpoint with the ufbl_get_entry_detail_action action to extract, modify, or escalate privileges within the WordPress database.	Patched by core rule	Y
CVE-2018-25351	Joomla EkRishta 2.10 Unauthenticated Error-Based SQL Injection	Joomla! Component EkRishta 2.10 contains an error-based SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code into the username parameter. Attackers can submit POST requests to the login endpoint with SQL injection payloads in the username field to extract database information including user credentials and system details.	Patched by core rule	Y
CVE-2018-25348	Joomla Ek Rishta 2.10 Unauthenticated SQL Injection (cid parameter)	Joomla! Component Ek Rishta 2.10 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the cid parameter. Attackers can send GET requests to the user_detail view with malicious cid values containing SQL commands to extract sensitive database information.	Patched by core rule	Y
CVE-2018-25347	WordPress Contact Form Maker Plugin 1.12.20 Authenticated SQL Injection	WordPress Contact Form Maker Plugin 1.12.20 contains SQL injection vulnerabilities that allow authenticated attackers to manipulate	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		database queries through the FormMakerSQLMapping and generete_csv_fmc AJAX actions. Attackers can inject malicious SQL code via the 'name' and 'search_labels' parameters to extract sensitive database information or escalate privileges.		
CVE-2018-25346	WordPress Form Maker Plugin (≤1.12.24) Authenticated SQL Injection	WordPress Form Maker Plugin 1.12.24 and below contains SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries by injecting SQL code through the FormMakerSQLMapping and generete_csv actions. Attackers can submit POST requests with malicious SQL payloads in the name and search_labels parameters to extract, modify, or escalate privileges within the WordPress database.	Patched by core rule	Y
CVE-2018-25342	Smartshop 1 Unauthenticated Time-Based Blind SQL Injection	Smartshop 1 contains a time-based blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'searched' parameter in search.php. Attackers can send GET requests with malicious SQL payloads like SLEEP commands to extract sensitive database information including product details and system data.	Patched by core rule	Y
CVE-2018-25341	Smartshop 1 Unauthenticated SQL Injection (id parameter)	Smartshop 1 contains a SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to product.php with union-based SQL injection payloads in the id parameter to extract sensitive database information including usernames and database names.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2018-25340	Smartshop 1 Unauthenticated SQL Injection (id parameter)	Smartshop 1 contains a SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to category.php with UNION-based SQL injection payloads in the id parameter to extract sensitive database information including usernames and other data.	Patched by core rule	Y
CVE-2026-9082	Drupal Core SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Drupal Drupal core allows SQL Injection. This issue affects Drupal core: from 8.9.0 before 10.4.10, from 10.5.0 before 10.5.10, from 10.6.0 before 10.6.9, from 11.0.0 before 11.1.10, from 11.2.0 before 11.2.12, from 11.3.0 before 11.3.10.	Patched by core rule	Y
CVE-2026-6379	WP Photo Album Plus (< 9.1.11.001) Unauthenticated SQL Injection	The WP Photo Album Plus WordPress plugin before 9.1.11.001 does not properly sanitize and escape a parameter before using it in a SQL query, allowing unauthenticated users to perform SQL injection attacks.	Patched by core rule	Y
CVE-2018-25339	Zechat 1.5 Time-Based Blind SQL Injection (v parameter)	Zechat 1.5 contains a SQL injection vulnerability in the v parameter that allows unauthenticated attackers to extract database information using time-based blind techniques. Attackers can exploit the v parameter with sleep-based blind injection to confirm vulnerability and extract data.	Patched by core rule	Y
CVE-2018-25338	Zechat 1.5 Union-Based SQL Injection (hashtag parameter)	Zechat 1.5 contains a SQL injection vulnerability in the hashtag parameter that allows unauthenticated attackers to extract database information using union-based techniques. Attackers can exploit the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		hashtag parameter with union-based payloads to retrieve table and column names.		
CVE-2018-25333	Nordex Wind Turbine Web Server 4.0 Unauthenticated SQL Injection	Nordex N149/4.0-4.5 Wind Turbine Web Server 4.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the login parameter in login.php. Attackers can submit crafted POST requests with SQL injection payloads in the login field to extract sensitive database information and bypass authentication mechanisms.	Patched by core rule	Y
CVE-2018-25330	Joomla EkRishta 2.10 Persistent XSS and SQL Injection	Joomla! extension EkRishta 2.10 contains persistent cross-site scripting and SQL injection vulnerabilities that allow attackers to inject malicious code through profile fields and POST parameters. Attackers can inject script payloads in profile information fields like Address that execute when users visit the profile, or submit SQL injection payloads via the phone_no parameter to the user_setting endpoint to manipulate database queries.	Patched by core rule	Y
CVE-2018-25319	Redaxo CMS Addon MyEvents 2.2.1 Authenticated SQL Injection	Redaxo CMS Addon MyEvents 2.2.1 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the myevents_id parameter. Attackers can send GET requests to the event_add.php page with malicious myevents_id values to extract or modify sensitive database information.	Patched by core rule	Y
CVE-2021-47980	Fuel CMS 1.4.13 Authenticated Blind SQL Injection	Fuel CMS 1.4.13 contains a blind SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the 'col' parameter in the Activity Log interface. Attackers can send requests to the logs endpoint with malicious SQL payloads in the 'col' parameter to extract database information based on response time delays.		
CVE-2021-47956	EgavilanMedia PHPCRUD 1.0 Unauthenticated SQL Injection	EgavilanMedia PHPCRUD 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the firstname parameter. Attackers can send POST requests to insert.php with malicious firstname values to extract sensitive database information.	Patched by core rule	Y
CVE-2021-47954	LayerBB 1.1.4 Unauthenticated SQL Injection	LayerBB 1.1.4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the search_query parameter. Attackers can send POST requests to /search.php with malicious search_query values using CASE WHEN statements to extract sensitive database information.	Patched by core rule	Y
CVE-2020-37244	Supsystic Membership 1.4.7 Unauthenticated SQL Injection	Supsystic Membership 1.4.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'search' and 'sidx' parameters. Attackers can send GET requests to the badges module with crafted payloads to extract sensitive database information using time-based blind or UNION-based SQL injection techniques.	Patched by core rule	Y
CVE-2020-37243	Supsystic Pricing Table 1.8.7 Unauthenticated SQL Injection	Supsystic Pricing Table 1.8.7 contains an SQL injection vulnerability in the 'sidx' GET parameter that allows unauthenticated attackers to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execute arbitrary SQL queries through the getListForTbl action. The plugin also contains stored cross-site scripting vulnerabilities in the 'Edit name' and 'Edit HTML' fields that execute malicious scripts when viewing pricing tables.		
CVE-2020-37242	Supsystic Ultimate Maps 1.1.12 Unauthenticated SQL Injection	Supsystic Ultimate Maps 1.1.12 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'sidx' GET parameter. Attackers can send crafted requests to the getListForTbl action with boolean-based blind or time-based blind SQL injection payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2021-47966	PHP Timeclock 1.04 Unauthenticated Blind SQL Injection	PHP Timeclock 1.04 contains time-based and boolean-based blind SQL injection vulnerabilities in the login_userid parameter of login.php that allows unauthenticated attackers to extract database contents. Attackers can submit crafted POST requests with SQL payloads using SLEEP functions or RLIKE conditional statements to dump sensitive database information including employee names and credentials.	Patched by core rule	Y
CVE-2020-37226	Joomla J2 JOBS 1.3.0 Authenticated SQL Injection (sortby parameter)	Joomla J2 JOBS 1.3.0 contains an authenticated SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the 'sortby' parameter. Attackers can send POST requests to the administrator index with malicious 'sortby' values to extract sensitive database	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		information using automated tools.		
CVE-2020-37224	Joomla J2 JOBS 1.3.0 Authenticated SQL Injection (sortby parameter)	Joomla J2 JOBS 1.3.0 contains an authenticated SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the 'sortby' parameter. Attackers can send POST requests to the administrator index with malicious 'sortby' values to extract sensitive database information.	Patched by core rule	Y
CVE-2020-37218	Joomla com_hdwplayer 4.2 Unauthenticated SQL Injection	Joomla com_hdwplayer 4.2 contains an SQL injection vulnerability in the search.php file that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the hdwplayersearch parameter. Attackers can submit POST requests with crafted SQL payloads in the hdwplayersearch parameter to extract sensitive database information from the hdwplayer_videos table.	Patched by core rule	Y
CVE-2021-47941	WordPress Survey & Poll Plugin 1.5.7.3 Unauthenticated SQL Injection via Cookie	WordPress Plugin Survey & Poll 1.5.7.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the wp_sap cookie parameter. Attackers can craft SQL payloads in the cookie to extract sensitive database information including usernames, passwords, and other confidential data from the WordPress database.	Patched by core rule	Y
CVE-2021-47930	Balbooa Joomla Forms Builder 2.0.6 Unauthenticated SQL Injection	Balbooa Joomla Forms Builder 2.0.6 contains an unauthenticated SQL injection vulnerability in the form submission handler that allows remote attackers to execute arbitrary SQL queries. Attackers can send POST	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		requests to the com_baforms component with malicious JSON payloads in the 'id' field parameter to extract sensitive database information.		
CVE-2021-47928	Opencart TMD Vendor System 3.x Unauthenticated Blind SQL Injection	Opencart TMD Vendor System 3.x contains a blind SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting SQL code through the product_id parameter. Attackers can craft malicious SQL queries using time-based or content-based blind injection techniques to enumerate usernames, emails, and password reset codes from the oc_user table.	Patched by core rule	Y
CVE-2026-41496	PraisonAI Multi-Agent System Vulnerability	PraisonAI is a multi-agent teams system. Prior to praisonai version 4.6.9 and praisonaiagents version 1.6.9, the fix for CVE-2026-40315 added input validation to SQLiteConversationStore only. Nine sibling backends ,Äî MySQL, PostgreSQL, async SQLite/MySQL/PostgreSQL, Turso, SingleStore, Supabase, SurrealDB ,Äî pass table_prefix straight into f-string SQL. Same root cause, same code pattern, same exploitation. 52 unvalidated injection points across the codebase. postgres.py additionally accepts an unvalidated schema parameter used directly in DDL. This issue has been patched in praisonai version 4.6.9 and praisonaiagents version 1.6.9.	Patched by core rule	Y
CVE-2026-4935	OttoKit WordPress Plugin (< 1.1.23) Unauthenticated SQL Injection	The OttoKit: All-in-One Automation Platform WordPress plugin before 1.1.23 does not properly sanitize user input before using it in a SQL statement, which could allow unauthenticated attackers to perform SQL injection attacks.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-46453	GL.iNet Firmware 4.x Authentication Bypass via SQL Injection	Certain GL.iNet devices with 4.x firmware allow authentication bypass (resulting in administrative control of the device) via a username that is both a valid SQL statement and a valid regular expression. For example, this affects version 4.3.7 on GL-MT3000 GL-AR300M GL-B1300 GL-AX1800 GL-AR750S GL-MT2500 GL-AXT1800 GL-X3000 and GL-SFT1200.	Patched by core rule	Y
CVE-2024-33722	SOPlanning 1.52.00 Authenticated SQL Injection	SOPlanning 1.52.00 is vulnerable to SQL Injection by an authenticated user via projets.php with statut[].	Patched by core rule	Y
CVE-2024-33288	Prison Management System PHP v1.0 SQL Injection on Admin Login	Prison Management System Using PHP v1.0 was discovered to contain a SQL injection vulnerability via the username on the Admin login page.	Patched by core rule	Y
CVE-2026-42208	LiteLLM LLM Gateway SQL Injection	LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. From version 1.81.16 to before version 1.83.7, a database query used during proxy API key checks mixed the caller-supplied key value into the query text instead of passing it as a separate parameter. An unauthenticated attacker could send a specially crafted Authorization header to any LLM API route (for example POST /chat/completions) and reach this query through the proxy's error-handling path. An attacker could read data from the proxy's database and may be able to modify it, leading to unauthorised access to the proxy and the credentials it manages. This issue has been patched in version 1.83.7.	Patched by core rule	Y
CVE-2026-41641	NocoBase No-Code Platform SQL Injection	NocoBase is an AI-powered no-code/low-code platform for building business applications	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and enterprise solutions. Prior to version 2.0.39, the checkSQL() validation function that blocks dangerous SQL keywords (e.g., pg_read_file, LOAD_FILE, dblink) is applied on the collections:create and sqlCollection:execute endpoints but is entirely missing on the sqlCollection:update endpoint. An attacker with collection management permissions can create a SQL collection with benign SQL, then update it with arbitrary SQL that bypasses all validation, and query the collection to execute the injected SQL and exfiltrate data. This issue has been patched in version 2.0.39.		
CVE-2026-41640	NocoBase No-Code Platform SQL Injection	NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to version 2.0.39, the queryParentSQL() function in the core database package constructs a recursive CTE query by joining nodeIds with string concatenation instead of using parameterized queries. The nodeIds array contains primary key values read from database rows. An attacker who can create a record with a malicious string primary key can inject arbitrary SQL when any subsequent request triggers recursive eager loading on that collection. This issue has been patched in version 2.0.39.	Patched by core rule	Y
CVE-2026-33324	SQLBot Text-to-SQL System SQL Injection	SQLBot is an intelligent Text-to-SQL system based on large language models and RAG. In versions 1.7.0 and earlier, the Text2SQL chat interface is vulnerable to prompt injection. The user-provided question parameter is directly concatenated into the LLM prompt without filtering or escaping, and the SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		extracted from the LLM response is executed against the database without validation or sanitization. An authenticated attacker can craft a malicious question to manipulate the LLM into generating and executing arbitrary SQL statements. When connected to a PostgreSQL data source, this can lead to remote code execution via COPY FROM PROGRAM. This issue has been fixed in version 1.7.1.		
CVE-2026-38428	Kestra (≤v1.3.3) SQL Injection	Kestra v1.3.3 and before is vulnerable to SQL Injection. The vulnerability occurs because user-controlled input from a GET parameter is directly concatenated into an SQL query without proper sanitization or parameterization. As a result, attackers can inject arbitrary SQL expressions into the database query.	Patched by core rule	Y
CVE-2026-42087	OpenC3 COSMOS Embedded Systems Platform SQL Injection	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems. From version 6.7.0 to before version 7.0.0-rc3, a SQL injection vulnerability exists in the Time-Series Database (TSDB) component of COSMOS. The tsdb_lookup function in the cvt_model.rb file directly places user-supplied input into a SQL query without sanitizing the input. As a result, a user can break out of the initial SQL statement and execute arbitrary SQL commands, including deleting data. This issue has been patched in version 7.0.0-rc3.	Patched by core rule	Y
CVE-2018-25300	XATABoost CMS 1.0.0 Unauthenticated Union-Based SQL Injection	XATABoost CMS 1.0.0 contains a union-based SQL injection vulnerability that allows unauthenticated attackers to manipulate	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		database queries by injecting SQL code through the id parameter. Attackers can send GET requests to news.php with malicious id values to extract sensitive database information.		
CVE-2026-42167	ProFTPD mod_sql (< 1.3.9a) Remote Code Execution via SQL Injection	mod_sql in ProFTPD before 1.3.9a allows remote attackers to execute arbitrary code via a username, in scenarios where there is logging of USER requests with an expansion such as %U, and the SQL backend allows commands (e.g., COPY TO PROGRAM).	Patched by core rule	Y
CVE-2021-36438	Sourcecodester Online Job Portal SQL Injection	SQL Injection vulnerability exists in Sourcecodester Online Job Portal phppdo 1.0 ivia the category parameter in /jobportal/index.php.	Patched by core rule	Y
CVE-2026-26980	Ghost CMS Content API SQL Injection	Ghost CMS contains a SQL injection vulnerability in its Content API that allows unauthenticated or low-privileged remote attackers to manipulate database queries. The Content API endpoint improperly neutralizes user-supplied input before embedding it in SQL statements, enabling attackers to craft malicious request parameters that extract, modify, or delete data from the underlying database. Successful exploitation can expose published and draft post content, member email addresses, API keys, and other sensitive CMS data. AppTrana's core WAF rules detect and block SQL injection payloads targeting this vector.	Patched by core rule	Y

VULNERABILITY DETAILS

Server-Side Request Forgery (SSRF) Vulnerabilities

SSRF vulnerabilities allow attackers to induce the server to make HTTP requests to arbitrary internal or external targets, enabling internal network reconnaissance, cloud metadata exfiltration, and lateral movement. All 31 SSRF CVEs in May 2026 are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-47076	Hackney HTTP Client Library Server-Side Request Forgery	Interpretation Conflict vulnerability in benoitc hackney allows Server Side Request Forgery. hackney_url:normalize/2 URL-decodes the host component after the URL has been parsed into a #hackney_url{} record. OTP's uri_string:parse/1 and inet:parse_address/1 do not decode percent-escapes in the host, so a URL such as http://%31%32%37%2E%30%2E%30%2E%31/ is seen by a caller's allowlist validator with host %31%32%37%2E%30%2E%30%2E%31 (not an IP address), which passes the allowlist check. hackney's normalizer then decodes the host to 127.0.0.1 and opens a TCP connection to loopback. Because hackney:request/5 always calls hackney_url:normalize/2 with no opt-out, every request that takes a binary or list URL is affected. The same technique reaches cloud instance metadata services (169.254.169.254), RFC1918 networks, and any admin interface listening on localhost. This issue affects hackney: from 0.13.0 before 4.0.1.	Patched by core rule	Y
CVE-2026-33637	Faraday HTTP Client Library SSRF	Faraday is an HTTP client library abstraction layer that provides a common	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		interface over many adapters. Versions 2.0.0 through 2.14.1 still allow protocol-relative host override when the request target is passed as a URI object (rather than a String) to Faraday::Connection#build_exclusive_url. This bypasses the February 2026 fix for GHSA-33mh-2634-fwr2 and enables off-host request forgery: a request built from a fixed-base Faraday::Connection can be redirected to an attacker-controlled host, forwarding connection-scoped values such as Authorization headers and default query parameters. This issue has been fixed in version 2.14.3.		
CVE-2026-45245	Summarize Extension (< 0.15.1) Authenticated SSRF via Synthetic Mouseover	Summarize prior to 0.15.1 contains a vulnerability in the hover summary feature that allows malicious pages to dispatch synthetic mouseover events over attacker-controlled links, causing the extension to make authenticated daemon requests using stored tokens without verifying event trustworthiness. Attackers can place local or private-network URLs behind hoverable links to route authenticated requests through the daemon, potentially accessing sensitive internal endpoints when users interact with attacker-controlled content.	Patched by core rule	Y
CVE-2026-8768	Vercel AI (≤3.0.97) Vulnerability	A vulnerability was found in vercel ai up to 3.0.97. The affected element is the function validateDownloadUrl of the file packages/provider-utils/src/download-blob.ts of the component provider-utils. The manipulation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		results in server-side request forgery. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-45347	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.5.11, there is a blind server side request forgery (SSRF) via the PDF generate function. In the PDF export, user inputs are interpreted as HTML and embedded into the PDF. According to tests, scripts and some potentially dangerous tags (iFrame, Object, etc.) are blocked, preventing server-side content from being read through this vulnerability. However, an image tag can be used to force a server-side request (SSRF), as shown in the following below. This vulnerability is fixed in 0.5.11.	Patched by core rule	Y
CVE-2026-45338	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, a Server-Side Request Forgery (SSRF) vulnerability exists in _process_picture_url() in backend/open_webui/utils/oauth.py (line ~1338). The function fetches arbitrary URLs from OAuth picture claims without applying validate_url(), allowing an attacker to force the server to make HTTP requests to internal resources and exfiltrate the full response. This vulnerability is fixed in 0.9.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-45317	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.3, an application-wide Cross-Site Request Forgery (CSRF) vulnerability was found Open-WebUl's image uploading functionality. An attacker can set an image URL to a malicious endpoint, allowing them to perform actions on behalf of a victim user. Any authenticated user can exploit this vulnerability, and any user who views the compromised image (e.g., a profile picture) will unknowingly send a GET request to the attacker-controlled URL. This can lead to cookie theft, denial of service (DoS), or other malicious actions. This vulnerability is fixed in 0.9.3.	Patched by core rule	Y
CVE-2026-45401	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, the validate_url() function in backend/open_webui/retrieval/web/utils.py only validates the initial URL submitted by the caller. The HTTP clients used downstream (sync requests, async aiohttp, langchain's WebBaseLoader) follow HTTP 3xx redirects by default and do not re-validate the redirect target against the private-IP / metadata-IP block list. Any authenticated user can therefore submit a public URL that 302-redirects to an internal address (e.g. 127.0.0.1, 169.254.169.254, RFC1918) and read the internal response body via the /api/v1/retrieval/process/w	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		eb endpoint, the /api/v1/images/... endpoints, the /api/chat/completions endpoint with an image_url content part, and any other route that calls these helpers. This vulnerability is fixed in 0.9.5.		
CVE-2026-45400	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.5, a parsing difference between the urlparse and requests libraries led to an SSRF bypass vulnerability. This vulnerability is fixed in 0.9.5.	Patched by core rule	Y
CVE-2026-45331	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, validate_url() in backend/open_webui/retrieval/web/utils.py calls validators.ipv6(ip, private=True), but the validators library does NOT implement the private keyword for IPv6 ,Äî the call raises a ValidationError (which is falsy in a boolean context), so every IPv6 address passes the filter. In addition, IPv4-mapped IPv6 (::ffff:10.0.0.1) bypasses the IPv4 check entirely, and several reserved IPv4 ranges (0.0.0.0/8, 100.64.0.0/10, 192.0.0.0/24, etc.) are not blocked. This vulnerability is fixed in 0.9.0.	Patched by core rule	Y
CVE-2021-47958	CouchCMS 2.2.1 Authenticated SSRF via SVG File Upload	CouchCMS 2.2.1 contains a server-side request forgery vulnerability that allows authenticated attackers to make arbitrary HTTP requests by uploading malicious SVG files. Attackers can upload SVG files containing external	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		entity references through the browse.php endpoint to access internal services and resources.		
CVE-2026-44430	MCP Registry Server-Side Request Forgery	The MCP Registry provides MCP clients with a list of MCP servers, like an app store for MCP servers. Prior to 1.7.7, the Registry's HTTP-based namespace verification (POST /v0/auth/http, POST /v0.1/auth/http) uses safeDialContext (internal/api/handlers/v0/auth/http.go:67-110) to refuse dialling private/internal addresses when fetching the well-known public-key file from a publisher-supplied domain. The blocklist (isBlockedIP, lines 125-133) relies entirely on Go stdlib's IsLoopback / IsPrivate / IsLinkLocalUnicast / IsMulticast / IsUnspecified plus a manual CGNAT range. None of these cover IPv6 6to4 (2002::/16), NAT64 (64:ff9b::/96 and 64:ff9b:1::/48 per RFC 8215), or deprecated site-local (fec0::/10) ,Äî all of which encode arbitrary IPv4 in the address bits and tunnel to RFC1918 / cloud-metadata services on dual-stack / NAT64-enabled hosts. This vulnerability is fixed in 1.7.7.	Patched by core rule	Y
CVE-2026-42596	Gotenberg PDF API SSRF	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.31.0, the default deny-lists used by Gotenberg's downloadFrom feature and webhook feature are bypassable. Because the filter is regex-based and case-sensitive, an unauthenticated attacker can supply URLs such as http://[::ffff:127.0.0.1]:...	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and reach loopback or private HTTP services that the default deny-list is intended to block. This crosses a real security boundary because an external caller can force the server to make outbound requests to internal-only targets. This vulnerability is fixed in 8.31.0.		
CVE-2026-42595	Gotenberg PDF API SSRF	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.32.0, Gotenberg's Chromium URL-to-PDF endpoint (/forms/chromium/convert/url) has no default protection against HTTP/HTTPS-based SSRF. The default deny-list regex only blocks file:// URIs. An unauthenticated attacker can point Chromium at any internal IP ,Äî including loopback, RFC 1918 ranges, and cloud metadata endpoints ,Äî and receive the response rendered as a PDF. Additionally, even when operators configure a custom deny-list, the protection is bypassed via HTTP redirects. Gotenberg's Chromium instance follows 302 redirects from an attacker-controlled external URL to internal targets without re-validating the redirect destination against the deny-list. This vulnerability is fixed in 8.32.0.	Patched by core rule	Y
CVE-2026-42591	Gotenberg PDF API SSRF	Gotenberg is a Docker-powered stateless API for PDF files. Prior to 8.32.0, the LibreOffice conversion endpoint (/forms/libreoffice/convert) passes uploaded documents directly to LibreOffice without inspecting their content. LibreOffice then fetches any embedded	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		external URLs on its own, completely bypassing the SSRF filters. This vulnerability is fixed in 8.32.0.		
CVE-2026-42281	MagicMirror² Smart Mirror Platform SSRF	MagicMirror¬≤ is an open source modular smart mirror platform. Prior to 2.36.0, an unauthenticated Server-Side Request Forgery (SSRF) vulnerability in the /cors endpoint allows any remote attacker to force the MagicMirror¬≤ server to perform arbitrary HTTP requests to internal networks, cloud metadata services, and localhost services. The endpoint also expands environment variable placeholders (**VAR_NAME**), enabling exfiltration of server-side secrets. This vulnerability is fixed in 2.36.0.	Patched by core rule	Y
CVE-2026-5773	libcurl SMB/SMBS Wrong Connection Reuse Vulnerability	libcurl might in some circumstances reuse the wrong connection for SMB(S) transfers. libcurl features a pool of recent connections so that subsequent requests can reuse an existing connection to avoid overhead. When reusing a connection a range of criteria must be met. Due to a logical error in the code, a network transfer operation that was requested by an application could wrongfully reuse an existing SMB connection to the same server that was using a different 'share' than the new subsequent transfer should. This could in unlucky situations lead to the download of the wrong file or the upload of a file to the wrong place. When this happens, the same credentials are used and the server name is the same.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-44015	Nginx UI Web Interface SSRF	Nginx UI is a web user interface for the Nginx web server. In 2.3.4 and earlier, an authenticated user can perform Server-Side Request Forgery (SSRF) by creating a cluster node pointing to an arbitrary internal URL and then sending API requests with the X-Node-ID header. The Proxy middleware forwards these requests to the attacker-specified internal address, bypassing network segmentation and enabling access to services bound to localhost or internal networks.	Patched by core rule	Y
CVE-2026-43995	Flowise LLM UI Builder SSRF	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, multiple tool implementations directly import and invoke raw HTTP clients (node-fetch, axios) instead of using the secured wrapper. These tools include (1) OpenAPIToolkit/OpenAPIToolkit.ts, (2) WebScraperTool/WebScraperTool.ts, (3) MCP/core.ts, and (4) Arxiv/core.ts. This vulnerability is fixed in 3.1.0.	Patched by core rule	Y
CVE-2026-42860	Open edX Enterprise Service SSRF	The Open edx Enterprise Service app provides enterprise features to the Open edX platform. From 7.0.2 to 7.0.4, the sync_provider_data endpoint in SAMLProviderDataViewSet fetches SAML metadata from a URL stored in SAMLProviderConfig.metadata_source. An authenticated user with the Enterprise Admin role can set this field to an arbitrary URL via the SAMLProviderConfigViewSet PATCH endpoint, then trigger a server-side HTTP	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		request by calling sync_provider_data. The fetch in fetch_metadata_xml() passes the URL directly to requests.get() with no scheme enforcement, IP filtering, or timeout. This vulnerability is fixed in 7.0.5.		
CVE-2026-42858	Open edX Platform SSRF	Open edX Platform enables the authoring and delivery of online learning at any scale. The sync_provider_data endpoint in SAMLProviderDataViewSet allows authenticated Enterprise Admin users to supply an arbitrary URL via the metadata_url POST parameter. This URL is passed directly to requests.get() in fetch_metadata_xml() without any URL validation, IP filtering, or scheme enforcement. An attacker with Enterprise Admin privileges can force the server to make HTTP requests to internal network services, cloud metadata endpoints (e.g., AWS 169.254.169.254), or other attacker-controlled destinations. This vulnerability is fixed by commit 6fda1f120ff5a590d120ae1180185525f399c6d0 and 70a56246dd9c9df57c596e64bdd8a11b1d9da054.	Patched by core rule	Y
CVE-2026-2393	MLflow (< 3.9.0) Server-Side Request Forgery	A Server-Side Request Forgery (SSRF) vulnerability exists in MLflow versions prior to 3.9.0. The `_create_webhook()` function in `mlflow/server/handlers.py` accepts a user-controlled `url` parameter without validation, and the `_send_webhook_request()` function in `mlflow/webhooks/delivery.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		py` sends HTTP POST requests to this attacker-controlled URL. This allows an authenticated attacker to force the MLflow backend to send HTTP requests to internal services, cloud metadata endpoints, or arbitrary external servers. The lack of input sanitization, URL scheme filtering, or allowlist validation on the webhook URL enables exploitation, potentially leading to cloud credential theft, internal network access, and data exfiltration.		
CVE-2026-42339	New API LLM Gateway SSRF	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. In versions 0.11.9-alpha.1 and prior, the SSRF protection introduced in v0.9.0.5 (CVE-2025-59146) and hardened in v0.9.6 (CVE-2025-62155) does not block the unspecified address 0.0.0.0. A regular (non-admin) user holding any valid API token can send a multimodal request to /v1/chat/completions, /v1/responses, or /v1/messages with 0.0.0.0 as the image/file URL host, bypassing the private-IP filter and causing the server to issue HTTP requests to localhost. This constitutes at minimum a blind SSRF; when the request is routed through an AWS/Bedrock Claude adaptor, the fetched content is inlined into the model response, upgrading it to a full-read SSRF. At time of publication, there are no publicly available patches.	Patched by core rule	Y
CVE-2026-44335	PraisonAI Multi-Agent System SSRF	PraisonAI is a multi-agent teams system. Prior to version 1.6.32, the URL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		checking logic in PraisonAI has a logical flaw that could be bypassed by attackers, leading to SSRF attacks. This issue has been patched in version 1.6.32.		
CVE-2026-42261	PromptHub AI Toolbox SSRF	PromptHub is an all-in-one AI toolbox for prompt, skill, and agent management. From version 0.4.9 to before version 0.5.4, apps/web/src/routes/skills.ts exposes an authenticated endpoint POST /api/skills/fetch-remote that fetches a user-supplied URL server-side and reflects the response body (up to 5 MB) back to the caller. The SSRF protection in apps/web/src/utils/remote-http.ts (isPrivateIPv6) attempts to block private/loopback destinations, but multiple alternate-but-valid IPv6 representations bypass the check. The bypasses reach any IPv4 address (loopback, RFC1918, link-local) via IPv4-mapped IPv6 in hex form, and the canonical ::1 via any representation that isn't the literal string "::1". Any authenticated user (role: user or admin) can trigger the SSRF. On deployments configured with ALLOW_REGISTRATION=true ,Äî a supported and documented configuration ,Äî this means any internet user who can register. This issue has been patched in version 0.5.4.	Patched by core rule	Y
CVE-2026-39383	Gotenberg Document Conversion API SSRF	Gotenberg is an API-based document conversion tool. In version 8.29.1, an unauthenticated attacker with network access can force the server to make outbound HTTP POST requests to arbitrary internal	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		or external destinations by supplying a crafted URL in the Gotenberg-Webhook-Url request header. The FilterDeadline function in filter.go is intended to gate outbound URLs, but when both the allow-list and deny-list are empty (the default configuration), it returns nil unconditionally and permits any URL. This is a blind SSRF: Gotenberg POSTs the converted document to the webhook URL and only checks whether the response status code is an error, but never returns the target's response body to the attacker. An attacker can use this to probe internal network infrastructure by observing whether the error callback is invoked, force POST requests against internal services that perform side effects, and confirm reachability of cloud metadata endpoints. The retryable HTTP client issues up to 4 automatic retries per request, amplifying each probe. This issue has been fixed in version 8.31.0. As a workaround, configure the GOTENBERG_API_WEBHOOK_ALLOW_LIST environment variable to restrict webhook URLs to known receivers, or set GOTENBERG_API_WEBHOOK_DENY_LIST to block RFC-1918 and link-local address ranges.		
CVE-2026-40280	Gotenberg Document Conversion API SSRF	Gotenberg is an API-based document conversion tool. In versions 8.30.1 and earlier, the default private-IP deny-lists for the --webhook-deny-list and --api-download-from-deny-list flags use a case-sensitive regular expression	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		(^https?://) to match URL schemes. Because Go's net/url.Parse() normalizes the scheme to lowercase before establishing the outbound TCP connection, an attacker can bypass the deny-list by simply capitalizing part of the URL scheme (e.g., HTTP://, HTTPS://, or Http://). This allows unauthenticated requests to reach internal network services, including private IP ranges, loopback addresses, and cloud instance metadata endpoints such as HTTP://169.254.169.254/latest/meta-data/. This bypasses the same security control that was patched in CVE-2026-27018. This issue has been fixed in version 8.31.0.		
CVE-2026-7178	ChatGPTNextWeb NextChat (≤2.16.1) Weakness	A weakness has been identified in ChatGPTNextWeb NextChat up to 2.16.1. This affects the function storeUrl of the file app/api/artifacts/route.ts of the component Artifacts Endpoint. This manipulation of the argument ID causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2026-7177	ChatGPTNextWeb NextChat (≤2.16.1) Security Flaw	A security flaw has been discovered in ChatGPTNextWeb NextChat up to 2.16.1. Affected by this issue is the function proxyHandler of the file app/api/[provider]/[...path]/route.ts. The manipulation results in server-side request forgery. The attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		may be performed from remote. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2026-7094	ShadowCloneLabs GlutamateMCPServers SSRF	A vulnerability was determined in ShadowCloneLabs GlutamateMCPServers up to e2de73280b01e5d943593dd1aa2c01c5b9112f78. Affected by this issue is some unknown functionality of the file src/puppeteer/index.ts of the component puppeteer_navigate. Executing a manipulation of the argument url can lead to server-side request forgery. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2026-44578	Next.js React Framework SSRF	Next.js contains a server-side request forgery (SSRF) vulnerability affecting the framework's built-in image optimization and data fetching layers. When user-controlled URLs are passed to Next.js API routes or server-side helpers without adequate validation, an attacker can coerce the application server into issuing outbound HTTP requests to internal network addresses, cloud metadata endpoints (e.g.,	Patched by core rule	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		169.254.169.254), or arbitrary external destinations. This enables exfiltration of instance credentials, internal service enumeration, and data leakage. Coverage has been added to AppTrana's core rule set to identify and block SSRF payloads targeting Next.js deployments.		

VULNERABILITY DETAILS

Cross-Site Scripting (XSS) Vulnerabilities

Cross-site scripting vulnerabilities allow attackers to inject malicious scripts into web pages, enabling session hijacking, credential theft, and full remote code execution. With 98 CVEs, XSS was the largest attack category in May 2026. All are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2018-25349	userSpice 4.3.24 Stored XSS via X-Forwarded-For Header	userSpice 4.3.24 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts through the X-Forwarded-For HTTP header. Attackers can send crafted requests to the backup.php endpoint with XSS payloads in the X-Forwarded-For header that execute when administrators visit the audit log page.	Patched by core rule	Y
CVE-2026-4929	Drupal 7 Simple Hierarchical Select (SHS) Cross-Site Scripting	Simple Hierarchical Select (SHS) for Drupal 7 contains cross-site scripting risk due to improper output escaping of term-derived text. Confirmed affected paths include field formatter output (shs_field_formatter_view) and term-tree child-term data generation (shs_term_get_children). Malicious taxonomy term names can be rendered unsafely depending on output context. This affects versions from 7.x-1.0 through (and including) 7.x-1.10.	Patched by core rule	Y
CVE-2026-4093	Drupal 7 Term Reference Tree Module Stored XSS	In the Drupal 7 Term Reference Tree module, two stored XSS vectors exist in the widget/formatter rendering pipeline. Vector A (token display templates): When the Token module is enabled and token display templates are configured, attacker-controlled token output (e.g., term description) is rendered	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		without proper sanitization. Any user who can edit the referenced taxonomy terms can inject HTML/JS that executes when the field is rendered. Vector B (term label rendering): Taxonomy term labels are not properly sanitized before being rendered in the widget, allowing a user with permission to create or edit taxonomy terms to inject scripts into the term name that execute when a form containing the widget is viewed. Exploit affects versions 7.x-1.x up to and including 7.x-1.11.		
CVE-2026-5776	Email Encoder WordPress Plugin (< 2.4.7) Unauthenticated Stored XSS	The Email Encoder WordPress plugin before 2.4.7 does not escape email addresses retrieved via user input, allowing unauthenticated attackers to perform Stored XSS attacks	Patched by core rule	Y
CVE-2026-33741	EspoCRM CRM Application Cross-Site Scripting	EspoCRM is an open source customer relationship management application. Versions 9.3.3 and below allow authenticated users to upload SVG attachments through normal attachment-capable fields and later serve those SVG files as top-level inline documents through both the attachment and image entry points, resulting in stored cross-user XSS reachable through a normal attachment workflow. Although inline SVG script is blocked by the response CSP, the same CSP still allows same-origin external script. As a result, an attacker can upload a malicious SVG together with a second attacker-controlled JavaScript attachment, then trick another user into opening the SVG to execute JavaScript in the victim's EspoCRM origin. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		has been fixed in version 9.3.4.		
CVE-2026-6495	Ajax Load More WordPress Plugin (< 7.8.4) Reflected XSS	The Ajax Load More WordPress plugin before 7.8.4 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-2026-3220	Autoptimize / Clearfy Cache / Speed Optimizer WordPress Plugins Unauthenticated Stored XSS	The Autoptimize WordPress plugin before 3.1.15, Clearfy Cache WordPress plugin before 2.4.2, Speed Optimizer WordPress plugin before 7.7.9 are vulnerable to unauthenticated Stored Cross-Site Scripting (XSS) due to a predictable replacement hash used during the HTML minification process and abusing a regular expression. This allows an attacker to inject arbitrary HTML attributes in the final HTML output by anticipating the placeholder format.	Patched by core rule	Y
CVE-2018-25331	Zenar CMS Unauthenticated Cross-Site Scripting	Zenar Content Management System contains a cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating form parameters in POST requests. Attackers can inject script tags through the current_page parameter sent to the ajax.php endpoint, which reflects unsanitized user input in the response HTML to execute arbitrary JavaScript in victim browsers.	Patched by core rule	Y
CVE-2021-47981	Quick.CMS 6.7 Authenticated Stored XSS in Sliders Form	Quick.CMS 6.7 contains a cross-site scripting vulnerability in the sliders form that allows authenticated attackers to inject malicious scripts by submitting XSS payloads through the sDescription parameter. Attackers can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		craft CSRF forms targeting the admin.php?p=sliders-form endpoint to execute arbitrary JavaScript in victim browsers when the form is submitted.		
CVE-2021-47975	WP Learn Manager 1.1.2 Unauthenticated Stored XSS	WP Learn Manager 1.1.2 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts through the `fieldtitle` parameter. Attackers can submit POST requests to the jslm_fieldordering page with XSS payloads in the fieldtitle field to execute arbitrary JavaScript when administrators view the field ordering interface.	Patched by core rule	Y
CVE-2021-47957	Cookie Law Bar 1.2.1 Authenticated Stored XSS	Cookie Law Bar 1.2.1 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting unsanitized input to the Bar Message field. Attackers can inject script payloads through the plugin settings page that execute in the browsers of all WordPress users viewing the site, enabling cookie theft and sensitive data exfiltration.	Patched by core rule	Y
CVE-2021-47955	CouchCMS 2.2.1 Authenticated XSS via SVG File Upload	CouchCMS 2.2.1 contains a cross-site scripting vulnerability that allows authenticated attackers to execute arbitrary JavaScript by uploading malicious SVG files through the file upload functionality. Attackers can upload SVG files containing embedded script tags to the browse.php endpoint, which are then executed in users' browsers when the files are accessed or previewed.	Patched by core rule	Y
CVE-2021-47934	MyBB Timeline Plugin 1.0 Cross-Site Scripting	MyBB Timeline Plugin 1.0 contains cross-site scripting vulnerabilities that allow	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers to inject malicious scripts through thread titles, post content, and user profile fields like Location and Bio. Attackers can also exploit a cross-site request forgery vulnerability in the timeline.php profile action to change a user's cover picture by crafting malicious forms that execute when victims visit affected profiles.		
CVE-2020-37245	Supsystic Digital Publications 1.6.9 Path Traversal	Supsystic Digital Publications 1.6.9 contains a path traversal vulnerability in the Folder input field that allows attackers to access files outside the web root by injecting directory traversal sequences. Additionally, the plugin fails to sanitize input fields in publication settings, allowing stored cross-site scripting attacks through script injection in parameters like Area Width and Publication Width that execute when publications are viewed or edited.	Patched by core rule	Y
CVE-2020-37240	Queue Management System 4.0.0 Authenticated Stored XSS	Queue Management System 4.0.0 contains a stored cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts through user creation fields. Attackers can insert JavaScript payloads in the First Name, Last Name, and Email fields during user creation, which execute when viewing the User List page.	Patched by core rule	Y
CVE-2020-37238	CMS Made Simple 2.2.15 Authenticated Stored XSS via SVG Upload	CMS Made Simple 2.2.15 contains a stored cross-site scripting vulnerability that allows authenticated users with Content Manager access to inject malicious scripts through SVG file uploads. Attackers can upload SVG files containing embedded JavaScript to the file manager, which executes	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		when other authenticated users access the uploaded file, enabling cookie theft and session hijacking.		
CVE-2020-37237	Composr CMS 10.0.34 Authenticated Persistent XSS in Banner Management	Composr CMS 10.0.34 contains a persistent cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts through the banner management interface. Attackers with admin credentials can inject XSS payloads in the Description field of the Add banner functionality, which execute for all website visitors when they access the home page.	Patched by core rule	Y
CVE-2020-37236	NewsLister Authenticated Persistent XSS (title parameter)	NewsLister contains an authenticated persistent cross-site scripting vulnerability that allows authenticated administrators to inject malicious scripts through the title parameter in the news addition interface. Attackers can inject JavaScript payloads via the title field in the admin panel that execute when news items are viewed by other users.	Patched by core rule	Y
CVE-2020-37235	WordPress Wibar Theme 1.1.8 Authenticated Stored XSS (Logo URL)	WordPress Theme Wibar 1.1.8 contains a stored cross-site scripting vulnerability in the Brand component that allows authenticated users to inject malicious scripts by manipulating the Logo URL parameter. Attackers with editor, administrator, contributor, or author privileges can inject base64-encoded script payloads through the ftc_brand_url input field to execute arbitrary JavaScript when users visit the brand page.	Patched by core rule	Y
CVE-2020-37233	WordPress BuddyPress 6.2.0 Authenticated Persistent XSS	WordPress Plugin Buddypress 6.2.0 contains a persistent cross-site scripting vulnerability that allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		authenticated attackers with moderator privileges to inject malicious script code through the figure parameter in wp:html blocks. Attackers can inject iframe elements with event handlers like onload that execute when administrators or privileged users preview or view the affected page content, enabling session hijacking and persistent phishing attacks.		
CVE-2026-45665	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.0, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Banner component due to an improper sanitization order (specifically, DOMPurify is executed before the marked library). This vulnerability allows a compromised or malicious administrator to plant a malicious payload in the global banner. Crucially, this vector enables Privilege Escalation, as the malicious banner is rendered for all users, including the Super Admin (Primary Admin). Consequently, the payload successfully bypasses the existing security mechanism. An attacker can leverage this to steal the Super Admin's session token This vulnerability is fixed in 0.8.0.	Patched by core rule	Y
CVE-2026-45318	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.3, his advisory tracks a regression of the original Excel-preview XSS (CVE-2026-44549). The same root cause ,Äî XLSX.utils.sheet_to_html() output rendered via {@html excelHtml} without DOMPurify ,Äî was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		reintroduced sometime after v0.8.0 and is exploitable again This vulnerability is fixed in 0.9.3.		
CVE-2026-45315	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.3, the audio transcription upload endpoint takes the file extension from the user-supplied filename and saves the file under CACHE_DIR/audio/transcriptions/.. The /cache/{path} route serves these files via FileResponse, which sets Content-Type from the on-disk extension and emits no Content-Disposition. A verified user with the default-on chat.stt permission can upload a polyglot WAV+HTML file named pwn.html and trick any other user into opening the resulting URL ,Äî the response comes back as text/html and any embedded <script> runs in the Open WebUI origin. This vulnerability is fixed in 0.9.3.	Patched by core rule	Y
CVE-2026-45303	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.5, through the HTML rendering view, scripts can be injected and executed. The frontend provides a function to visualize the HTML content of a current chat. The content is embedded in an iFrame with the allow-scripts allow-forms allow-same-origin sandbox directive. This means that the content is placed in a sandbox but with permission to execute scripts and access the parent,Äôs data (e.g., local storage). As a result, only a few functions are restricted (e.g., displaying an alert box), but in effect, the sandbox attribute is largely	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		nullified. This vulnerability is fixed in 0.6.5.		
CVE-2026-44549	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.0, Excel file attachments are previewed in an unsafe way. A crafted XLSX file payload can be used to cause the sheetjs function sheet_to_html to embed an XSS payload into the generated HTML. This is subsequently added to the DOM unsanitized via @html causing the payload to trigger. This vulnerability is fixed in 0.8.0.	Patched by core rule	Y
CVE-2026-44721	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, a stored cross-site scripting (XSS) vulnerability that allows any authenticated user with model creation permission (workspace.models) to execute arbitrary JavaScript in the browser of any other user (including admins) who views the malicious model in the chat UI. This vulnerability is fixed in 0.9.0.	Patched by core rule	Y
CVE-2026-44568	Open WebUI AI Platform Vulnerability	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.0, the AccountPending.svelte component renders the admin-configured "Pending User Overlay Content" using marked.parse() inside {@html} with an incorrect DOMPurify application order. An admin can inject arbitrary JavaScript into the Pending User Overlay Content that executes in the browser context of any pending user who views the overlay page.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is fixed in 0.9.0.		
CVE-2021-47968	Podcast Generator 3.1 Authenticated Persistent XSS	Podcast Generator 3.1 is vulnerable to persistent cross-site scripting, allowing authenticated attackers to inject malicious scripts by submitting unfiltered JavaScript code in the long_description parameter. Attackers can inject script tags through episode creation or editing requests to execute arbitrary JavaScript when other users view the episode details.	Patched by core rule	Y
CVE-2021-47967	PHP Timeclock 1.04 Unauthenticated Cross-Site Scripting	PHP Timeclock 1.04 contains multiple cross-site scripting vulnerabilities that allow unauthenticated attackers to inject arbitrary JavaScript by manipulating URL paths and POST parameters. Attackers can append malicious payloads to login.php, timeclock.php, audit.php, and timerpt.php endpoints, or inject code through from_date and to_date parameters in report requests to execute scripts in user browsers.	Patched by core rule	Y
CVE-2021-47963	Anote 1.0 Persistent XSS via Malicious Markdown Files	Anote 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to execute arbitrary code by injecting malicious payloads into markdown files stored within the application. Attackers can craft malicious markdown files with embedded JavaScript that executes system commands when opened, enabling remote code execution on the victim's computer.	Patched by core rule	Y
CVE-2021-47962	Savsoft Quiz 5.0 Authenticated Persistent XSS in Account Settings	Savsoft Quiz 5.0 contains a persistent cross-site scripting vulnerability in the user account settings page that allows authenticated attackers to inject malicious HTML and JavaScript code.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Attackers can inject script payloads into user profile fields at the edit_user endpoint, which execute in the browsers of users viewing the affected profile after submission.		
CVE-2026-44429	MCP Registry Cross-Site Scripting	The MCP Registry provides MCP clients with a list of MCP servers, like an app store for MCP servers. Prior to 1.7.7, the public catalogue UI served at GET / (file internal/api/handlers/v0/ui_index.html) is vulnerable to stored cross-site scripting via the server.websiteUrl field of any published server.json. Server-side validation in internal/validators/validators.go (validateWebsiteURL) only checks that the URL parses, is absolute, and uses the https scheme; it does not reject quote characters. Client-side, the value is interpolated into a double-quoted href attribute via innerHTML, using a homegrown escapeHtml helper that performs the standard textContent ,Üí innerHTML round-trip. Per the HTML serialisation algorithm, that round-trip encodes only &, <, > and U+00A0 inside text nodes ,Äî it does not encode " or '. A literal " in websiteUrl therefore breaks out of the href attribute, allowing arbitrary on* event handlers to be appended to the same <a> element. The Content-Security-Policy on / is script-src 'self' 'unsafe-inline' https://cdn.tailwindcss.com, so the injected event handlers execute. Any user able to obtain a publish token (e.g. via POST /v0/auth/github-at with their own GitHub account, or POST /v0/auth/none on a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		deployment that has anonymous auth enabled) can plant a poisoned record visible to every visitor of the registry homepage. This vulnerability is fixed in 1.7.7.		
CVE-2026-42897	Microsoft Exchange Server XSS / Spoofing	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	Patched by core rule	Y
CVE-2026-42159	Flowsint OSINT Tool Cross-Site Scripting	Flowsint is an open-source OSINT graph exploration tool designed for cybersecurity investigation, transparency, and verification. Prior to 1.2.3, Flowsint allows a user to create investigations, which are used to manage sketches and analyses. Sketches have controllable graphs, which are comprised of nodes and relationships. The sketches contain information on an OSINT target (usernames, websites, etc) within these nodes and relationships. A remote attacker can create a node with a malicious description that contains arbitrary HTML. When the node is selected, it will render the arbitrary HTML, potentially triggering stored XSS. This vulnerability is fixed in 1.2.3.	Patched by core rule	Y
CVE-2026-43644	podinfo (≤6.11.2) Reflected XSS in /echo and /api/echo Endpoints	podinfo through 6.11.2 contains a reflected cross-site scripting vulnerability in the /echo and /api/echo endpoints where the echoHandler writes request body content directly to the response without setting explicit Content-Type or X-Content-Type-Options headers. Attackers can craft cross-origin HTML pages with auto-submitting forms containing script payloads in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the request body, which are served as text/html due to Go's content type detection, allowing the reflected script to execute in the podinfo origin context when victims visit the attacker's page.		
CVE-2020-37225	Powie's WHOIS Domain Check 0.9.31 Authenticated Persistent XSS	Powie's WHOIS Domain Check 0.9.31 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject arbitrary JavaScript by exploiting unsanitized input fields in plugin settings. Attackers can submit malicious payloads through textarea and input elements in the pwhois_settings.php configuration page to execute JavaScript in the admin context and escalate privileges.	Patched by core rule	Y
CVE-2020-37222	Kuicms PHP EE 2.0 Unauthenticated Persistent XSS	Kuicms Php EE 2.0 contains a persistent cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted content through the bbs reply endpoint. Attackers can send POST requests to /web/?c=bbs&a=reply with HTML and JavaScript payloads in the content parameter to execute arbitrary scripts in users' browsers.	Patched by core rule	Y
CVE-2020-37174	WOOF Products Filter for WooCommerce 1.2.3 Authenticated Persistent XSS	WOOF Products Filter for WooCommerce 1.2.3 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by entering XSS payloads in design tab textfields. Attackers can inject JavaScript code through fields like 'Text for block toggle' and 'Custom front css styles' that executes on frontend pages when	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		saved, affecting all site visitors.		
CVE-2026-44245	Kyverno Cloud Native Policy Engine Vulnerability	Kyverno is a policy engine designed for cloud native platform engineering teams. Prior to 2.5.2, Vue 3's v-html directive is the framework-documented mechanism for injecting raw HTML, and it intentionally disables the auto-escaping that {{ }} interpolation provides. The PropertyCard.vue component uses v-html for the else branch of the URL check, meaning any non-URL string value flows directly into the DOM as HTML. The isURL() guard only filters values that parse as http: or https: URLs, so any HTML payload not starting with those schemes bypasses it entirely. The data originates from Kubernetes PolicyReport .results[].properties fields, which are arbitrary string maps populated by policy engines and potentially by any principal with write access to PolicyReport objects in the cluster. This vulnerability is fixed in 2.5.2.	Patched by core rule	Y
CVE-2026-42338	ip-address JavaScript Library Vulnerability	ip-address is a library for parsing and manipulating IPv4 and IPv6 addresses in JavaScript. Prior to 10.1.1, Address6.group() and Address6.link() do not HTML-escape attacker-controlled content before embedding it in the HTML strings they return, and AddressError.parseMessage (emitted by the Address6 constructor for invalid input) can contain unescaped attacker-controlled content in one branch. An application that (1) passes untrusted input to Address6 and (2) renders the output of these methods, or the thrown error's parseMessage, as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		HTML (e.g. via innerHTML) is vulnerable to cross-site scripting. This vulnerability is fixed in 10.1.1.		
CVE-2026-42554	Fiber Go Web Framework Vulnerability	Fiber is a web framework for Go. Prior to 2.52.12 and 3.1.0, Cross-Site Scripting vulnerability in Go Fiber allows a remote attacker to inject arbitrary HTML/JavaScript by supplying Accept: text/html on any request whose handler passes attacker-influenced data to the AutoFormat() feature. The developer opts into content negotiation by calling AutoFormat(), but does not opt into raw HTML emission for a particular request; Fiber chooses that branch from attacker-controlled Accept. The html branch is the sole outlier in a method whose name (AutoFormat) and symmetrical structure actively telegraph "safe, format-agnostic reply." This vulnerability is fixed in 2.52.12 and 3.1.0.	Patched by core rule	Y
CVE-2026-42857	Open edX Platform Cross-Site Scripting	Open edX Platform enables the authoring and delivery of online learning at any scale. The HTML sanitizer clean_thread_html_body() used for discussion notification emails fails to remove <style> tags from user-generated discussion post content. This content is rendered with Django's |safe template filter in email notification templates, allowing any enrolled student to inject arbitrary CSS into email notifications sent to other users. This enables email tracking (IP address disclosure), content spoofing, and phishing attacks. This vulnerability is fixed with commit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cddc25cd791bb78f76833896e4778f668861df12.		
CVE-2026-7814	pgAdmin 4 Browser Tree and Explain Visualizer Stored XSS	Stored cross-site scripting (XSS) vulnerability in pgAdmin 4 Browser Tree and Explain Visualizer modules. User-controlled PostgreSQL object names (database, schema, table, column, etc.) were assigned to DOM elements via innerHTML, allowing crafted object names containing HTML markup to execute attacker-supplied JavaScript in the browser of any pgAdmin user who navigated to or executed EXPLAIN over the malicious object. Fix replaces innerHTML with textContent. This issue affects pgAdmin 4: before 9.15.	Patched by core rule	Y
CVE-2026-42841	Grav File-Based Web Platform Vulnerability	Grav is a file-based Web platform. Prior to 2.0.0-beta.2, an authenticated user with page editing permissions can inject an executable JavaScript event-handler attribute into rendered image HTML through Grav's Markdown media action syntax. The issue is caused by Markdown image query parameters being converted into callable media actions. The public attribute() media method can be reached this way, allowing an editor to set an arbitrary HTML attribute name and value on the generated image element. This vulnerability is fixed in 2.0.0-beta.2.	Patched by core rule	Y
CVE-2026-42612	Grav File-Based Web Platform Vulnerability	Grav is a file-based Web platform. Prior to 2.0.0-beta.2, a stored Cross-Site Scripting (XSS) vulnerability in getgrav/grav allows publisher-level accounts to execute arbitrary JavaScript. The issue arises from a blacklist bypass in the detectXss() function when	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		handling unquoted HTML event attributes. This vulnerability is fixed in 2.0.0-beta.2.		
CVE-2026-42611	Grav File-Based Web Platform Vulnerability	Grav is a file-based Web platform. Prior to 2.0.0-beta.2, a low-privileged (with the ability to create a page) user can cause XSS with the injection of svg element. The XSS can further be escalated to dump the entire system information available under /admin/config/info whenever a Super Admin visits the page; which can further be chained with the use of admin-nonce to do a complete server compromise (RCE). This vulnerability is fixed in 2.0.0-beta.2.	Patched by core rule	Y
CVE-2022-50970	WordPress AAWP Plugin 3.16 Authenticated Reflected XSS	WordPress Plugin AAWP 3.16 contains a reflected cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by manipulating the tab parameter. Attackers can craft URLs with XSS payloads in the tab parameter of the aawp-settings admin page to execute arbitrary JavaScript in the context of authenticated users.	Patched by core rule	Y
CVE-2022-50969	uBidAuction 2.0.1 Reflected XSS in Mailing Log Module	uBidAuction 2.0.1 contains a reflected cross-site scripting vulnerability in the backend/mailingLog/manage module. The date_created, date_from, date_to, and created_at parameters in the filter functionality are not properly sanitized, allowing remote attackers to inject malicious scripts via crafted GET requests that execute in victims' browsers.	Patched by core rule	Y
CVE-2022-50968	uBidAuction 2.0.1 Reflected XSS in Auctions Module	uBidAuction 2.0.1 contains a reflected cross-site scripting vulnerability in the auctions/manage module. The date_created, date_from, date_to, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		created_at parameters in the filter functionality are not properly sanitized, allowing remote attackers to inject malicious scripts via crafted GET requests that execute in victims' browsers.		
CVE-2022-50967	uBidAuction 2.0.1 Reflected XSS in Tickets Module	uBidAuction 2.0.1 contains a reflected cross-site scripting vulnerability in the tickets/manage module. The date_created, date_from, date_to, and created_at parameters in the filter functionality are not properly sanitized, allowing remote attackers to inject malicious scripts via crafted GET requests that execute in victims' browsers.	Patched by core rule	Y
CVE-2022-50966	uBidAuction 2.0.1 Reflected XSS in News Module	uBidAuction 2.0.1 contains a reflected cross-site scripting vulnerability in the news/manage module. The date_created, date_from, date_to, and created_at parameters in the filter functionality are not properly sanitized, allowing remote attackers to inject malicious scripts via crafted GET requests that execute in victims' browsers.	Patched by core rule	Y
CVE-2022-50965	uBidAuction 2.0.1 Reflected XSS in Posts Module	uBidAuction 2.0.1 contains a reflected cross-site scripting vulnerability in the posts/manage module. The date_created, date_from, date_to, and created_at parameters in the filter functionality are not properly sanitized, allowing remote attackers to inject malicious scripts via crafted GET requests that execute in victims' browsers.	Patched by core rule	Y
CVE-2022-50964	uBidAuction 2.0.1 Reflected XSS in My Auctions (Loose Status)	uBidAuction 2.0.1 contains a reflected cross-site scripting vulnerability in the auctions/myAuctions/status/loose module. The date_created, date_from, date_to, and created_at	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameters in the filter functionality are not properly sanitized, allowing remote attackers to inject malicious scripts via crafted GET requests that execute in victims' browsers.		
CVE-2022-50963	uBidAuction 2.0.1 Reflected XSS in My Auctions (Active Status)	uBidAuction 2.0.1 contains a reflected cross-site scripting vulnerability in the auctions/myAuctions/status/active module. The date_created, date_from, date_to, and created_at parameters in the filter functionality are not properly sanitized, allowing remote attackers to inject malicious scripts via crafted GET requests that execute in victims' browsers.	Patched by core rule	Y
CVE-2022-50962	uBidAuction 2.0.1 Reflected XSS in My Orders Module	uBidAuction 2.0.1 contains a reflected cross-site scripting vulnerability in the orders/myOrders module. The date_created, date_from, date_to, and created_at parameters in the filter functionality are not properly sanitized, allowing remote attackers to inject malicious scripts via crafted GET requests that execute in victims' browsers.	Patched by core rule	Y
CVE-2022-50961	WordPress IP2Location Country Blocker 2.26.7 Authenticated Stored XSS	WordPress Plugin IP2Location Country Blocker 2.26.7 contains a stored cross-site scripting vulnerability that allows authenticated users to inject arbitrary JavaScript code through the Frontend Settings interface. Attackers can inject malicious scripts in the URL field of the Display page settings that execute when administrators or other authenticated users visit the plugin settings page.	Patched by core rule	Y
CVE-2022-50960	WordPress International SMS for CF7 Plugin 1.2 Reflected XSS	WordPress International SMS for Contact Form 7 Integration version 1.2 contains a reflected cross-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		site scripting vulnerability in the page parameter of the admin settings interface. Attackers can inject malicious scripts through the page parameter in class-sms-log-display.php to execute arbitrary JavaScript in administrator browsers.		
CVE-2022-50959	WordPress Contact Form Builder 1.6.1 Unauthenticated Reflected XSS	WordPress Contact Form Builder 1.6.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by exploiting the form_id parameter. Attackers can craft malicious URLs to code_generator.php with script payloads in the form_id parameter to execute arbitrary JavaScript in victim browsers.	Patched by core rule	Y
CVE-2022-50958	WordPress Jetpack Plugin 9.1 Unauthenticated Reflected XSS	WordPress Plugin Jetpack 9.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the post_id parameter. Attackers can craft URLs to the grunion-form-view.php endpoint with script payloads in the post_id parameter to execute arbitrary JavaScript in victim browsers.	Patched by core rule	Y
CVE-2022-50957	Drupal avatar_uploader 7.x-1.0-beta8 Unauthenticated Reflected XSS	Drupal avatar_uploader 7.x-1.0-beta8 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the file parameter. Attackers can craft URLs with script payloads in the file parameter of avatar_uploader.pages.inc to execute arbitrary JavaScript in victim browsers.	Patched by core rule	Y
CVE-2022-50949	WordPress Videos sync PDF Plugin	WordPress Plugin Videos sync PDF 1.7.4 contains a stored cross-site scripting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.7.4 Authenticated Stored XSS	vulnerability that allows authenticated attackers to inject malicious scripts by exploiting unsanitized mov, pdf, mp4, webm, and ogg parameters. Attackers can inject payloads like autofocus onfocus event handlers through the plugin options panel to execute arbitrary JavaScript when administrators view or edit video settings.		
CVE-2022-50948	Motopress Hotel Booking Lite 4.2.4 Authenticated Stored XSS	Motopress Hotel Booking Lite 4.2.4 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting payloads in accommodation type fields. Attackers can inject script tags through the title and excerpt parameters when creating accommodation types, which execute in the browser when visitors access the accommodations page.	Patched by core rule	Y
CVE-2022-50947	WordPress Testimonial Slider and Showcase 2.2.6 Authenticated Stored XSS	WordPress Plugin Testimonial Slider and Showcase 2.2.6 contains a stored cross-site scripting vulnerability that allows authenticated editors to inject malicious scripts by failing to sanitize the post_title parameter. Attackers with editor privileges can inject JavaScript payloads through the testimonial title field that execute in the browsers of users viewing the draft post, enabling cookie theft and session hijacking.	Patched by core rule	Y
CVE-2022-50946	WordPress Netroics Blog Posts Grid 1.0 Authenticated Stored XSS	WordPress Plugin Netroics Blog Posts Grid 1.0 contains a stored cross-site scripting vulnerability that allows authenticated editors to inject malicious scripts by failing to sanitize the post_title parameter.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Attackers with editor privileges can inject script payloads through the testimonial title field that execute in the browsers of other users viewing the draft post, enabling cookie theft and session hijacking.		
CVE-2022-50945	WordPress 3dady Real-Time Web Stats Plugin 1.0 Authenticated Stored XSS	WordPress 3dady Real-Time Web Stats plugin 1.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious JavaScript by exploiting unsanitized input fields. Attackers can insert JavaScript payloads in the dady_input_text or dady2_input_text fields via the plugin options panel to execute arbitrary code when the page is viewed.	Patched by core rule	Y
CVE-2022-50943	Moodle LMS 4.0 Unauthenticated XSS via Search Parameter	Moodle LMS 4.0 contains a cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting payloads through the search parameter. Attackers can inject JavaScript code via the search field in course/search.php to execute arbitrary scripts in users' browsers and steal session cookies.	Patched by core rule	Y
CVE-2021-47951	WordPress Picture Gallery 1.4.2 Authenticated Stored XSS	WordPress Picture Gallery 1.4.2 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the Edit Content URL field in the Access Control settings. Attackers can enter JavaScript payloads in the plugin options that are stored in the database and executed when the functionality is triggered, enabling session hijacking or credential theft.	Patched by core rule	Y
CVE-2021-47950	Advanced Guestbook 2.4.4	Advanced Guestbook 2.4.4 contains a persistent cross-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Authenticated Persistent XSS in Smilies Admin	site scripting vulnerability in the smilies administration interface that allows authenticated attackers to inject malicious scripts by manipulating the s_emotion parameter. Attackers can submit POST requests to admin.php with JavaScript code in the s_emotion field, which executes when administrators view the smilies tab.		
CVE-2021-47948	WordPress GetPaid Plugin 2.4.6 Authenticated HTML Injection	WordPress GetPaid Plugin 2.4.6 contains an HTML injection vulnerability that allows authenticated attackers to inject arbitrary HTML code by exploiting the Help Text field in payment forms. Attackers can inject malicious HTML including image tags and scripts into the Help Text field during payment form creation, which gets stored in the database and executed in the browser when the form is viewed.	Patched by core rule	Y
CVE-2021-47947	Projectsend r1295 Authenticated Stored XSS (name parameter)	Projectsend r1295 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input in the 'name' parameter of files-edit.php. Attackers can inject JavaScript payloads through the file name field that execute in the browser when the file is viewed by other users, particularly affecting System Administrator users on the Dashboard page.	Patched by core rule	Y
CVE-2021-47931	Exponent CMS 2.6 Authenticated Stored XSS	Exponent CMS 2.6 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the Title and Text Block parameters in the text editing endpoint. Attackers can inject iframe payloads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with embedded SVG onload events to execute arbitrary JavaScript. The application also exposes database credentials in responses and lacks brute-force protection on authentication endpoints.		
CVE-2021-47929	Filterable Portfolio Gallery 1.0 Authenticated Stored XSS	Filterable Portfolio Gallery 1.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious JavaScript by entering payloads in the title field. Attackers can store JavaScript code like image tags with onerror handlers that execute when the gallery is previewed, affecting all users viewing the page.	Patched by core rule	Y
CVE-2021-47927	WordPress WP Symposium Pro 2021.10 Authenticated Stored XSS	WordPress Plugin WP Symposium Pro 2021.10 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by exploiting insufficient sanitization of the forum name parameter. Attackers can submit POST requests to the admin setup page with JavaScript payloads in the wps_admin_forum_add_name parameter, which are stored and executed when the forum is accessed.	Patched by core rule	Y
CVE-2021-47926	Contact Form to Email 1.3.24 Authenticated Stored XSS	Contact Form to Email 1.3.24 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by creating forms with script tags in the form name field. Attackers can craft form names containing JavaScript code that executes when other logged-in users access the form management page, enabling session hijacking or credential theft.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-47925	CMDBuild 3.3.2 Authenticated Stored XSS	CMDBuild 3.3.2 contains multiple stored cross-site scripting vulnerabilities that allow authenticated attackers to inject arbitrary web script or HTML via crafted input in card creation and file upload endpoints. Attackers can inject XSS payloads through Employee card parameters or SVG file attachments in the classes endpoint, which execute when other users view the affected records or preview attachments.	Patched by core rule	Y
CVE-2021-47924	Ultimate Product Catalogue 5.8.2 Authenticated Stored XSS (price parameter)	Ultimate Product Catalogue 5.8.2 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the price parameter. Attackers can submit POST requests to post.php with HTML/JavaScript payloads in the price field to execute arbitrary code when the product is viewed.	Patched by core rule	Y
CVE-2021-47922	Slider by Soliloquy 2.6.2 Authenticated Stored XSS (title parameter)	Slider by Soliloquy 2.6.2 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the title parameter. Attackers can add JavaScript payloads in the title field when creating or editing sliders, which executes in the browsers of users viewing the slider on both administrative and frontend pages.	Patched by core rule	Y
CVE-2021-47910	AccessPress Social Icons 1.8.2 Authenticated Stored XSS	AccessPress Social Icons 1.8.2 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by entering JavaScript payloads into the 'icon title' field. Attackers can store XSS payloads like image tags with onerror event handlers that execute when the plugin	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		page is viewed, affecting all users who access the plugin interface.		
CVE-2021-47907	Rocket LMS 1.1 Authenticated Persistent XSS in Support Ticket Module	Rocket LMS 1.1 contains a persistent cross-site scripting vulnerability in the support ticket module that allows authenticated users to inject malicious script code through the title parameter. Attackers can submit support tickets with embedded HTML/JavaScript payloads that execute in the browsers of other users viewing the message history, enabling session hijacking and phishing attacks.	Patched by core rule	Y
CVE-2026-6735	PHP FPM Status Page XSS (versions 8.2.x < 8.2.31, 8.3.x < 8.3.31, 8.4.x < 8.4.21, 8.5.x < 8.5.6)	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, 8.5.* before 8.5.6, due to improper sanitation of user data, it allows an attacker to compose an URL, which will cause the target to execute arbitrary JavaScript code (XSS) on the target's machine when the target is viewing the PHP-FPM status page.	Patched by core rule	Y
CVE-2024-33724	SOPlanning 1.52.00 Cross-Site Scripting (groupe_id parameter)	SOPlanning 1.52.00 is vulnerable to Cross Site Scripting (XSS) via the groupe_id parameter to process/groupe_save.php.	Patched by core rule	Y
CVE-2026-40296	PhpSpreadsheet XSS Vulnerability	PhpSpreadsheet is a pure PHP library for reading and writing spreadsheet files. The HTML writer skips htmlspecialchars escaping when a cell's formatted value differs from the original value. When a cell has a custom number format containing the text placeholder @ along with any additional literal characters (for example ". @", "@ ", or "x@"), the formatter replaces @ with the cell value and adds the extra characters, causing the formatted value to differ from the original and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		bypassing HTML escaping entirely. An attacker who can control the cell value and number format of an uploaded spreadsheet that is later converted to HTML and displayed to other users can achieve stored cross-site scripting. This issue is fixed in versions 5.7.0, 3.10.5, 2.4.5, 2.1.16, and 1.30.4.		
CVE-2026-35453	PhpSpreadsheet XSS Vulnerability	PhpSpreadsheet is a library for reading and writing spreadsheet files. In versions 1.30.3 and earlier, 2.0.0 through 2.1.15, 2.2.0 through 2.4.4, 3.3.0 through 3.10.4, and 4.0.0 through 5.6.0, the HTML Writer skips htmlspecialchars() output escaping when a cell uses a custom number format containing the @ text placeholder with additional literal text (e.g., @ "items"). The escaping is only applied when the formatted output strictly equals the original cell value. When the format code contains @ with quoted literal text, the formatter substitutes the raw cell value into the format string and returns early without invoking the escaping callback. An attacker who can control cell content in a spreadsheet processed by the HTML Writer can inject arbitrary HTML and JavaScript into the generated output. This issue has been fixed in versions 1.30.4, 2.1.16, 2.4.5, 3.10.5, and 5.7.0.	Patched by core rule	Y
CVE-2026-38432	ERPNext (≤v15.103.1) XSS in Email Template Engine	ERPNext v15.103.1 and before is vulnerable to Cross Site Scripting (XSS) in the Email Template engine. An attacker with permission to create or edit email templates can inject malicious JavaScript code that are executed on the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		victim's browser when the template is applied.		
CVE-2026-27694	Traccar GPS Tracking System Cross-Site Scripting	Traccar is an open source GPS tracking system. In org.traccar:traccar versions starting at 6.11.1 before 6.13.0, the email notification templates insert user-controlled device, geofence, and driver names into HTML email output without proper escaping. An attacker with low privileges can store crafted HTML in these fields, which is then rendered in notification emails sent to other users with access to the affected devices. This can lead to phishing or spoofed email content. This issue is fixed in version 6.13.0.	Patched by core rule	Y
CVE-2023-54349	AmazCart CMS 3.4 Unauthenticated Reflected XSS via Search	AmazCart CMS 3.4 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting payloads through the search functionality. Attackers can enter script tags in the search box to execute arbitrary JavaScript that fires when search history is viewed or results are displayed.	Patched by core rule	Y
CVE-2026-42138	Dify LLM App Development Platform Cross-Site Scripting	Dify is an open-source LLM app development platform. Prior to version 1.13.1, using the method POST /api/files/upload, any unauthenticated user can upload an SVG file with XSS. The method POST /v1/files/upload, which requires authentication through the application API, is also vulnerable. This issue has been patched in version 1.13.1.	Patched by core rule	Y
CVE-2026-42086	OpenC3 COSMOS Cross-Site Scripting	OpenC3 COSMOS provides the functionality needed to send commands to and receive data from one or more embedded systems.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Prior to version 7.0.0, the Command Sender UI uses an unsafe eval() function on array-like command parameters, which allows a user-supplied payload to execute in the browser when sending a command. This creates a self-XSS risk because an attacker can trigger their own script execution in the victim,Äôs session, if allowed to influence the array parameter input, for example via phishing. If successful, an attacker may read or modify data in the authenticated browser context, including session tokens in local storage. This issue has been patched in version 7.0.0.		
CVE-2026-37503	V2Board (≤1.7.4) Cross-Site Scripting	Cross-Site Scripting (XSS) in V2Board thru 1.7.4. The custom_html field in theme configuration is rendered using Blade unescaped output in public/theme/v2board/dashboard.blade.php. An admin can inject arbitrary JavaScript via the saveThemeConfig API. All site visitors execute the payload, enabling cookie theft, session hijacking, or phishing.	Patched by core rule	Y
CVE-2018-25309	MyBB Recent Threads 17.0 Persistent XSS via Thread Subject	MyBB Recent threads 17.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts by creating threads with crafted subject lines. Attackers can create threads with script tags in the subject parameter to execute arbitrary JavaScript in the browsers of all users viewing the index page.	Patched by core rule	Y
CVE-2026-40230	Helpy Knowledge Base Stored XSS in Doc Rendering	Helpy contains a stored cross-site scripting vulnerability in the knowledge base Doc rendering logic. An	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		authenticated attacker with admin or agent editor privileges can persist arbitrary HTML or JavaScript in the body field of a knowledge base Doc.This issue affects helpy: 2.8.0.		
CVE-2026-40229	Helpy Stored XSS in Post Author Display	Helpy contains a stored cross-site scripting vulnerability in the post author display logic. Any registered user can persist arbitrary HTML in their account name field and cause it to be rendered unescaped in public forum threads where they participate, in the admin ticket view, and in HTML notification emails sent to other users.This issue affects helpy: 2.8.0.	Patched by core rule	Y
CVE-2025-56537	OpenNebula v6.10.0.1 Stored XSS in Virtual Network Template	A stored cross-site scripting (XSS) vulnerability in opennebula v6.10.0.1 and fixed in v.7.0 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the virtual network template parameter.	Patched by core rule	Y
CVE-2025-56536	OpenNebula v6.10.0.1 Stored XSS in User Information	A stored cross-site scripting (XSS) vulnerability in opennebula v6.10.0.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the user information parameter.	Patched by core rule	Y
CVE-2025-56535	OpenNebula v6.10.0.1 XSS in Zone Attribute	A cross-site scripting (XSS) vulnerability in opennebula v6.10.0.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the zone attribute parameter.	Patched by core rule	Y
CVE-2025-56534	OpenNebula v6.10.0.1 XSS in Custom Authenticator Driver	A cross-site scripting (XSS) vulnerability in the custom authenticator driver of opennebula v6.10.0.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-5306	Check & Log Email WordPress Plugin (< 2.0.13) Unauthenticated Stored XSS	The Check & Log Email WordPress plugin before 2.0.13 does not properly handle email replacement, which could allow unauthenticated users to perform Stored XSS attacks when the email encoder setting is enabled	Patched by core rule	Y
CVE-2026-5362	Authenticated Stored XSS via Document Embed Editable	An authenticated attacker with permission to edit document content can store crafted HTML/JavaScript in a Document embed editable and cause script execution when the published page is rendered. This issue affects pimcore: v12.3.3.	Patched by core rule	Y

VULNERABILITY DETAILS

Malicious File Upload Vulnerabilities

File upload vulnerabilities allow attackers to upload and execute malicious files, commonly PHP web shells, by bypassing incomplete extension or MIME type blocklists. All 7 file upload CVEs in May 2026 are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2018-25359	Splinterware System Scheduler Pro 5.12 Insecure File Permissions – Privilege Escalation	Splinterware System Scheduler Pro 5.12 contains an insecure file permissions vulnerability that allows low-privilege users to escalate privileges by modifying service executable files. Attackers can rename the WService.exe file in the installation directory and replace it with a malicious executable that executes with LocalSystem privileges when the service is triggered.	Patched by core rule	Y
CVE-2026-45246	Summarize Extension (< 0.15.1) Insecure File Permissions – Credential Exposure	Summarize prior to 0.15.1 contains an insecure file permission vulnerability in the refresh-free configuration rewrite path that allows local users to read sensitive credentials by exploiting default filesystem permissions. When the refresh-free path rewrites the configuration file, it creates the replacement with default process umask permissions instead of preserving the original file permissions, exposing the config file containing API keys and provider credentials to other local users on shared Unix-like systems.	Patched by core rule	Y
CVE-2020-37227	HS Brand Logo Slider 2.1 Authenticated Unrestricted File Upload	HS Brand Logo Slider 2.1 contains an unrestricted file upload vulnerability that allows authenticated users to bypass client-side file extension validation by uploading arbitrary files. Attackers can intercept upload requests to the logoupload parameter in the admin interface and rename files to executable extensions	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		.php to achieve remote code execution.		
CVE-2021-47965	WordPress WP Super Edit Plugin (≤2.5.4) Unrestricted File Upload via FCKeditor	WordPress Plugin WP Super Edit 2.5.4 and earlier contains an unrestricted file upload vulnerability in the FCKeditor component that allows attackers to upload dangerous file types without validation. Attackers can upload arbitrary files through the filemanager upload endpoint to achieve remote code execution and complete system compromise.	Patched by core rule	Y
CVE-2021-47943	TextPattern CMS 4.8.7 Authenticated RCE via Malicious PHP File Upload	TextPattern CMS 4.8.7 contains a remote code execution vulnerability that allows authenticated attackers to execute arbitrary commands by uploading malicious PHP files through the file upload functionality. Attackers can upload a PHP shell via the Files section in the content area and execute commands by accessing the uploaded file at /textpattern/files/ with GET parameters passed to the system function.	Patched by core rule	Y
CVE-2021-47937	e107 CMS 2.3.0 Authenticated RCE via Malicious Theme File Upload	e107 CMS 2.3.0 contains a remote code execution vulnerability that allows authenticated users with theme installation permissions to execute arbitrary commands by uploading malicious theme files. Attackers can upload a crafted theme package through the theme.php endpoint that deploys a web shell to the e107_themes directory, then execute system commands via the payload.php script.	Patched by core rule	Y
CVE-2026-38751	OpenSTAManager (≤2.10) Arbitrary File Upload in Module Update Functionality	OpenSTAManager version 2.10 and earlier contains an arbitrary file upload vulnerability in the module update functionality (modules/aggiornamenti/upload_modules.php)	Patched by core rule	Y

VULNERABILITY DETAILS

Code Injection Vulnerabilities

Code injection vulnerabilities allow attackers to inject and execute arbitrary code within the application context. May 2026 recorded 29 code injection CVEs, all protected by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-8724	Dataease 2.10.20 Security Flaw	A security flaw has been discovered in Dataease 2.10.20. Impacted is the function SqlparserUtils.transFilter of the file SqlparserUtils.java of the component Data Dashboard. The manipulation results in sql injection. The attack may 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.	Patched by core rule	Y
CVE-2021-47952	python-jsonpickle 2.0.0 Remote Code Execution via Insecure Deserialization	python jsonpickle 2.0.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary Python commands by deserializing malicious JSON payloads containing py/repr objects. Attackers can craft JSON strings with py/repr directives that invoke the eval function during deserialization to execute arbitrary code.	Patched by core rule	Y
CVE-2026-44246	nnU-Net Semantic Segmentation Framework Vulnerability	nnU-Net is a semantic segmentation framework that automatically adapts its pipeline to a dataset. Prior to 2.4.1, the nnU-Net Issue Triage workflow in .github/workflows/issue-triage.yml is vulnerable to Agentic Workflow	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Injection. The workflow sets allowed_non_write_users : ${{ github.event.issue.user.login }}, which means any logged-in GitHub user who opens an issue can reach this agentic workflow with attacker-controlled content. Untrusted issue title and body content are embedded directly into the prompt of anthropics/claude-code-action, and the workflow then runs a command-capable Claude agent with permission to comment on and relabel the current issue via gh. Because this workflow is triggered automatically on issues.opened, an external attacker can submit a crafted issue that steers the agent beyond its intended issue-triage purpose and influences authenticated issue actions. This vulnerability is fixed in 2.4.1.		
CVE-2026-31236	llm CLI Tool (≤0.27.1) Code Injection via --functions Argument	The llm CLI tool thru 0.27.1 contains a critical code injection vulnerability via its --functions command-line argument. This argument is intended to allow users to provide custom Python function definitions. However, the tool directly executes the provided code using the unsafe exec() function without any sanitization, sandboxing, or security restrictions. An attacker can exploit this by crafting a malicious llm command with arbitrary Python code in the --functions	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument and using social engineering to trick a victim into running it. This leads to arbitrary code execution on the victim's system, potentially granting the attacker full control.		
CVE-2026-31233	Guardrails AI (≤0.6.7) Code Injection in Hub Package Installation	Guardrails AI thru 0.6.7 contains a code injection vulnerability (CWE-94) in its Hub package installation mechanism. When installing validator packages via guardrails hub install, the system retrieves a manifest from the Guardrails Hub and dynamically executes a script specified in the post_install field. The script path is constructed from untrusted manifest data and executed without proper validation or sanitization, allowing remote code execution. An attacker who can publish malicious packages to the Hub can inject arbitrary code that will be executed on any system where a victim installs the malicious package.	Patched by core rule	Y
CVE-2026-8346	D-Link DIR-816 1.10CNB05_R1B011D88210 Vulnerability	A vulnerability was detected in D-Link DIR-816 1.10CNB05_R1B011D88210. This affects the function portForward. Performing a manipulation of the argument ip_address results in command injection. The attack can be initiated remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-8345	D-Link DIR-816 1.10CNB05_R1B011D88210 Security Vulnerability	A security vulnerability has been detected in D-Link DIR-816 1.10CNB05_R1B011D88	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		210. Affected by this issue is the function sub_445E7C of the file /goform/singlePortForward. Such manipulation of the argument ip_address leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.		
CVE-2026-8344	D-Link DIR-816 1.10CNB05_R1B011D88210 Weakness	A weakness has been identified in D-Link DIR-816 1.10CNB05_R1B011D88210. Affected by this vulnerability is the function sub_445E7C of the file /goform/formDMZ.cgi. This manipulation causes command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-31253	Flash-Attention Insecure Deserialization in Checkpoint Loading	The flash-attention training framework thru commit e724e2588cbe754beb97cf7c011b5e7e34119e62 (2025-13-04) contains an insecure deserialization vulnerability (CWE-502) in its checkpoint loading mechanism. The load_checkpoint() function in checkpoint.py and the checkpoint loading code in eval.py use torch.load() without enabling the security-restrictive weights_only=True parameter. This allows the deserialization of arbitrary Python objects via the pickle module. An attacker can exploit this by providing a maliciously crafted checkpoint file. When a victim loads this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		checkpoint during model warmstarting or evaluation, arbitrary code is executed on the victim's system.		
CVE-2026-31252	CosyVoice Insecure Deserialization in Model Loading	CosyVoice thru commit 6e01309e01bc93bbeb83bdd996b1182a81aaf11e (2025-30-21) contains an insecure deserialization vulnerability (CWE-502) in its model loading component. The framework uses torch.load() to load model weight files (e.g., llm.pt, flow.pt, hift.pt) without enabling the security-restrictive weights_only=True parameter. This allows the deserialization of arbitrary Python objects via the pickle module. An attacker can exploit this by providing a malicious model directory containing specially crafted model files. When a victim starts the CosyVoice Web UI pointing to this directory, arbitrary code is executed on the victim's system during the model loading process.	Patched by core rule	Y
CVE-2022-50944	Aero CMS 0.0.1 Authenticated PHP Code Injection via File Upload	Aero CMS 0.0.1 contains a PHP code injection vulnerability that allows authenticated attackers to execute arbitrary PHP code by uploading malicious files through the image parameter. Attackers can upload PHP files with embedded code to the admin posts.php endpoint with source=add_post parameter, and the uploaded files are executed by the server.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-47935	Sentry 8.2.0 Authenticated RCE via Pickle Deserialization	Sentry 8.2.0 contains a remote code execution vulnerability that allows authenticated superusers to execute arbitrary commands by injecting malicious pickle-serialized objects through the audit log entry data parameter. Attackers can submit crafted POST requests to the admin audit log endpoint with base64-encoded compressed pickle payloads in the data field to achieve code execution with application privileges.	Patched by core rule	Y
CVE-2025-67486	Dolibarr ERP/CRM Vulnerability	Dolibarr is an enterprise resource planning (ERP) and customer relationship management (CRM) software package. Versions 22.0.2 and earlier contains an authenticated remote code execution vulnerability in the user extrafields functionality. User-controlled input from the "computed value" field is passed to PHP's `eval()` function without adequate sanitization, allowing authenticated administrators to execute arbitrary PHP code on the server. As of time of publication, no patched versions are available.	Patched by core rule	Y
CVE-2026-41512	ai-scanner AI Model Safety Scanner Vulnerability	ai-scanner is an AI model safety scanner built on NVIDIA garak. From version 1.0.0 to before version 1.4.1, there is a remote code execution vulnerability via JavaScript injection in `BrowserAutomation::PlaywrightService`. This issue has been patched in version 1.4.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-46507	yeti-platform Yeti (< 2.1.12) Server-Side Template Injection	A SSTI (server side template injection) vulnerability in the custom template export function in yeti-platform yeti before 2.1.12 allows attackers to execute code on the application server.	Patched by core rule	Y
CVE-2026-38431	ERPNext (≤v15.103.1) Server-Side Template Injection	ERPNext v15.103.1 and before is vulnerable to Server-Side Template Injection (SSTI). An attacker with permission to create or edit email templates can inject template expressions that are executed on the server when the template is rendered.	Patched by core rule	Y
CVE-2026-7705	JD Cloud JDCOS 4.5.1.r4518 Flaw	A flaw has been found in JD Cloud JDCOS 4.5.1.r4518. This vulnerability affects the function set_iptv_info of the file /jdcap of the component Service Interface. Executing a manipulation of the argument vid can lead to command injection. 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-2026-7692	Wavlink WL-WN570HA1 R70HA1 V1410_221110 Vulnerability	A vulnerability was detected in Wavlink WL-WN570HA1 R70HA1 V1410_221110. The affected element is the function ping_ddns of the file /cgi-bin/adm.cgi. Performing a manipulation of the argument DDNS results in command injection. The attack can be initiated remotely. The exploit is now public and may be used. Once again the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2026-7691	Wavlink WL-WN570HA1 R70HA1 V1410_221110 Security Vulnerability	A security vulnerability has been detected in Wavlink WL-WN570HA1 R70HA1 V1410_221110. Impacted is the function set_sys_cmd of the file /cgi-bin/adm.cgi. Such manipulation of the argument command leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Once again the vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-7690	Wavlink WL-WN570HA1 R70HA1 V1410_221110 Weakness	A weakness has been identified in Wavlink WL-WN570HA1 R70HA1 V1410_221110. This issue affects the function set_sys_adm of the file /cgi-bin/adm.cgi. This manipulation of the argument Username causes command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Once	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		again the vendors acted very professional and confirms, "that the WN570HA1 firmware version R70HA1 V1410_221110 has been removed from our website." This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2026-7669	sgl-project SGLang (≤0.5.9) Vulnerability	A vulnerability was detected in sgl-project SGLang up to 0.5.9. Impacted is the function get_tokenizer of the file python/sglang/srt/utils/hf_transformers_utils.py of the component HuggingFace Transformer Handler. The manipulation of the argument trust_remote_code with the input False as part of Boolean results in code injection. The attack can be executed remotely. A high complexity level is associated with this attack. The exploitability is considered difficult. In get_tokenizer(), when the caller passes trust_remote_code=False and HuggingFace transformers v5 returns a TokenizersBackend instance (the generic fallback for tokenizer classes not in the registry), SGLang silently re-invokes AutoTokenizer.from_pretrained with trust_remote_code=True, overriding the caller's explicit security setting. A model repository containing a malicious tokenizer.py referenced via auto_map in tokenizer_config.json will	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execute arbitrary Python in the SGLang process during this second call. No log line or warning is emitted. The override affects all current SGLang versions because transformers==5.3.0 is pinned in pyproject.toml. Both tokenizer_mode="auto" and tokenizer_mode="slow" are affected. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-7410	SourceCodester Pizzafy Ecommerce System 1.0 Vulnerability	A vulnerability has been found in SourceCodester Pizzafy Ecommerce System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=add_to_cart. The manipulation of the argument pid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-7409	SourceCodester Pizzafy Ecommerce System 1.0 Flaw	A flaw has been found in SourceCodester Pizzafy Ecommerce System 1.0. This affects the function save_user of the file /admin/ajax.php?action=save_user. Executing a manipulation can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-7408	SourceCodester Pizzafy Ecommerce System 1.0 Vulnerability	A vulnerability was detected in SourceCodester Pizzafy Ecommerce System 1.0. Affected by this issue is the function save_menu	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /admin/ajax.php?action=save_menu. Performing a manipulation results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.		
CVE-2026-7407	SourceCodester Pizzafy Ecommerce System 1.0 Security Vulnerability	A security vulnerability has been detected in SourceCodester Pizzafy Ecommerce System 1.0. Affected by this vulnerability is the function save_settings of the file /pizzafy/admin/ajax.php?action=save_settings of the component Setting Handler. Such manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-7160	Tenda HG3 2.0 Vulnerability	A vulnerability was determined in Tenda HG3 2.0. This vulnerability affects the function formTracert of the file /boaform/formTracert. Executing a manipulation of the argument datasize can lead to command injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-7102	Tenda F456 1.0.0.5 Vulnerability	A vulnerability was found in Tenda F456 1.0.0.5. This impacts the function FromWriteFacMac of the file /goform/WriteFacMac of the component httpd. The manipulation of the argument mac results in command injection. The attack can be executed remotely. The exploit has been made public and could be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-7067	D-Link DIR-822 A_101 Vulnerability	A vulnerability was determined in D-Link DIR-822 A_101. The impacted element is the function system of the file /udhcpcd/dhcpd.c of the component udhcpd DHCP Service. This manipulation of the argument Hostname causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-7023	ByteDance coze-studio (≤0.5.1) Vulnerability	A vulnerability was detected in ByteDance coze-studio up to 0.5.1. Affected by this vulnerability is the function ExecuteSQL of the file backend/domain/memory/database/service/database_impl.go of the component databaseTool. Performing a manipulation results in sql injection. The attack can be initiated 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

VULNERABILITY DETAILS

VULNERABILITY DETAILS

Design and Config Vulnerabilities

AppTrana core rules also blocked four CVEs spanning Security Misconfiguration, Authentication Failures, Logging and Monitoring Failures, and Insecure Design weaknesses, extending protection beyond injection-based attack patterns.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-54346	Backup Migration WordPress Plugin Unauthenticated Remote Code Execution (RCE)	The Backup Migration WordPress plugin versions 1.3.7 and earlier contain a critical unauthenticated remote code execution vulnerability in backup-heart.php. The file accepts a user-controlled content-dir parameter that is concatenated into a PHP require_once() path without validation or authentication checks. An unauthenticated remote attacker can supply a path to an attacker-controlled file, causing the server to include and execute arbitrary PHP code with web server privileges. Exploitation enables full server compromise, webshell deployment, credential harvesting, and lateral movement. The vulnerability was actively exploited in the wild before a patch was released in version 1.3.8.	Patched by core rule	Y
CVE-2026-44575	Next.js Middleware Authentication / Authorization Bypass	Next.js versions prior to 14.2.25 and 15.x prior to 15.2.3 contain an authentication and authorization bypass vulnerability in the middleware layer. When a Next.js application uses middleware to enforce access controls, an attacker can send a request with a crafted x-middleware-subrequest header that causes the middleware to be skipped	Patched by core rule	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		entirely, bypassing all authentication, authorization, and security checks defined within it. This allows unauthenticated and unprivileged users to access protected routes, admin panels, or API endpoints that should require valid credentials or specific roles. The flaw affects self-hosted deployments running Next.js in standalone or custom server mode and does not impact applications hosted on Vercel.		
CVE-2026-42945	NGINX Vulnerability (Infrastructure-Level Coverage)	A security vulnerability has been identified in NGINX affecting specific builds or modules of the web server software. The vulnerability enables remote attackers to achieve unauthorized outcomes—such as request smuggling, access control bypass, or code execution—by sending specially crafted HTTP requests that exploit improper request processing logic in the affected NGINX component. Exploitation conditions and impact vary depending on the deployment configuration, module set, and upstream service topology. Mitigation is enforced at the infrastructure layer through network access controls, updated NGINX builds, and hardened server configurations that neutralize the attack vector before requests reach application services.	Patched by core rule	Y
CVE-2026-9256	NGINX 'ngx-poolslip' Heap Buffer Overflow	NGINX contains a heap buffer overflow vulnerability, referred to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as 'ngx-poolslip', in its memory pool management routines. The flaw is triggered by sending a sequence of specially crafted HTTP requests that cause the NGINX worker process to write beyond the bounds of an allocated heap buffer. Depending on heap layout and server configuration, exploitation may result in denial of service through process crash, or—in more advanced scenarios—arbitrary code execution with the privileges of the NGINX worker. An unauthenticated remote attacker with network access to the NGINX listener can trigger this condition. Mitigation is applied at the infrastructure level by deploying a patched NGINX build and enforcing network-layer traffic filtering that limits exposure to untrusted request sources.		

INDUSFACE™

DALLAS | BENGALURU | VADODARA | MUMBAI | NEW DELHI

Contact Us: +1 866 458 3058, +91 265 6133021

sales@indusface.com | indusface.com