INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

December 2025

The total zero-day vulnerabilities count for December month: 253

Command Injection	SQLi	SSRF	Code Injection	XSS	Broken Access Control	Security Misconfiguration
30	35	11	72	85	9	11

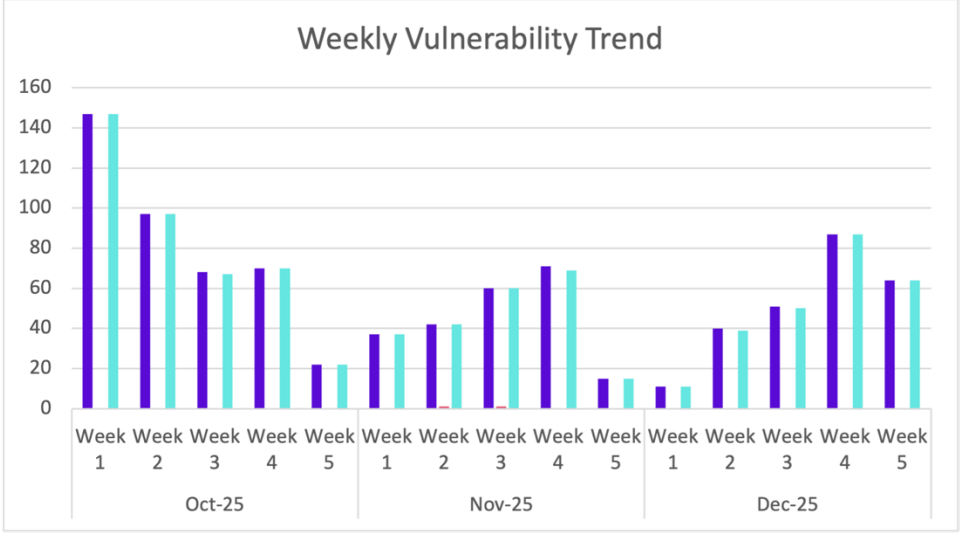
Zero-day vulnerabilities protected through core rules	253
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	251

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

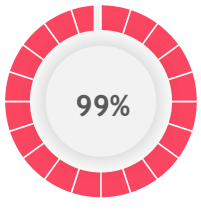
Vulnerability Trend:

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

Weekly Vulnerability Trend

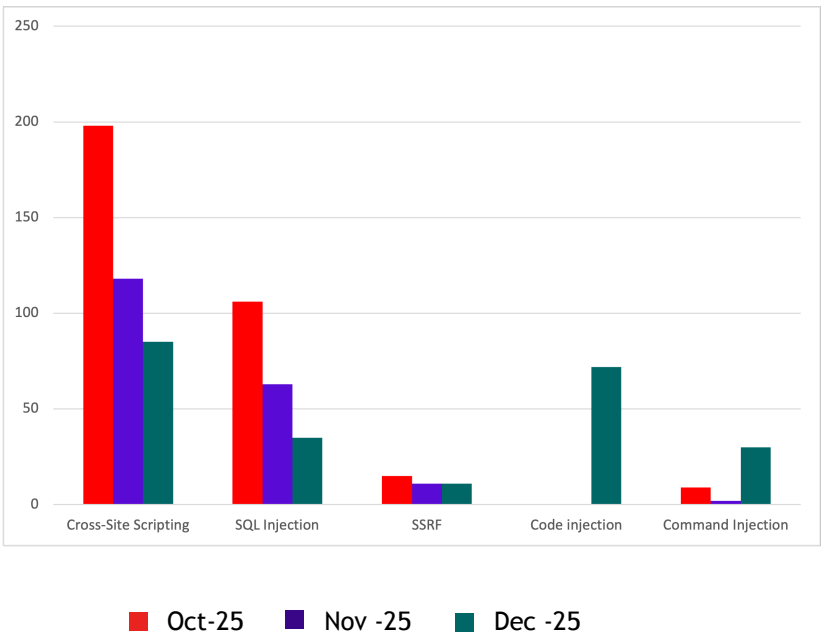


of the zero-day vulnerabilities were protected by the AppTrana core rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-43876	An OS Command Injection vulnerability that allows an attacker to potentially execute unauthorized commands on the system under certain circumstances.	Under certain circumstances a successful exploitation could result in access to the device.	Patched by core rule	Y
CVE-2025-43875	An OS Command Injection vulnerability that allows an attacker to potentially execute unauthorized commands on the system under certain circumstances.	Under certain circumstances a successful exploitation could result in access to the device.	Patched by core rule	Y
CVE-2025-66213	An OS Command Injection vulnerability that allows an attacker to potentially execute unauthorized commands on the system under certain circumstances.	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in the File Storage Directory Mount Path functionality allows users with application/service management permissions to execute arbitrary commands as root on managed servers. The file_storage_directory_source parameter is passed directly to shell commands without proper sanitization, enabling full remote code executio	Patched by core rule	Y
CVE-2025-66212	A command injection vulnerability in a privileged system component allowing arbitrary command execution.	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in the Dynamic Proxy Configuration	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Filename handling allows users with application/service management permissions to execute arbitrary commands as root on managed servers. Proxy configuration filenames are passed to shell commands without proper escaping, enabling full remote code execution. Version 4.0.0-beta.451 fi		
CVE-2025-66211	A remote command injection vulnerability in a service endpoint enabling unauthorized command execution.	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in PostgreSQL Init Script Filename handling allows users with application/service management permissions to execute arbitrary commands as root on managed servers. PostgreSQL initialization script filenames are passed to shell commands without proper validation, enabling full remote code execution. Version 4.0.0-beta.	Patched by core rule	Y
CVE-2025-66210	A critical command injection vulnerability in a backend module resulting in potential remote code execution.	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.451, an authenticated command injection vulnerability in the Database Import functionality allows users with application/service management permissions to execute arbitrary commands as root on managed servers. Database names used in import operations are passed directly to shell commands without sanitization, enabling full remote code execution. Version 4.0.0-beta.451 f	Patched by core rule	Y
CVE-2025-25364	A command injection vulnerability in the me.connectify.SMJobBlessHelper XPC service of Speedify VPN	A command injection vulnerability in the me.connectify.SMJobBlessHelper XPC service of Speedify VPN up to v15.0.0 allows attackers to execute arbitrary commands with root-level privileges.	Patched by core rule	Y
CVE-2025-29229	linksys E5600 V1.1.0.26 is vulnerable to command injection	linksys E5600 V1.1.0.26 is vulnerable to command injection in the function ddnsStatus.	Patched by core rule	Y
CVE-2025-29228	Linksys E5600 V1.1.0.26 is vulnerable to command injection	Linksys E5600 V1.1.0.26 is vulnerable to command injection in the runtime.macClone function via the mc.ip parameter.	Patched by core rule	Y
CVE-2025-50526	Netgear EX8000 V1.0.0.126 was discovered to contain a command injection vulnerability	Netgear EX8000 V1.0.0.126 was discovered to contain a command injection vulnerability via the switch_status function.	Patched by core rule	Y
CVE-2025-45493	Netgear EX8000 V1.0.0.126 is vulnerable to Command Injection	Netgear EX8000 V1.0.0.126 is vulnerable to Command Injection via the iface parameter in the action_bandwidth function.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-14388	The PhastPress plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Read	The PhastPress plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Read via null byte injection in all versions up to, and including, 3.7. This is due to a discrepancy between the extension validation in `getExtensionForURL()` which operates on URL-decoded paths, and `appendNormalized()` which strips everything after a null byte before constructing the filesystem path. This makes it possible for unauthenticated attackers to read arbitrary files from the webroot, including wp-con	Patched by core rule	Y
CVE-2023-53981	Command injection vulnerability	PhotoShow 3.0 contains a remote code execution vulnerability that allows authenticated administrators to inject malicious commands through the exiftran path configuration. Attackers can exploit the ffmpeg configuration settings by base64 encoding a reverse shell command and executing it through a crafted video upload process.	Patched by core rule	Y
CVE-2025-11774	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the software keyboard function (hereinafter referred to as "keypad function") of Mitsubishi Electric GENESIS64 versions 10.97.2 CFR3 and prior, Mitsubishi Electric Iconics Digital Solutions GENESIS64 versions 10.97.2 CFR3 and prior, Mitsubishi Electric ICONICS Suite versions 10.97.2 CFR3 and prior, Mitsubishi Electric Iconics Digital Solutions ICONICS Suite versions 10.97.2 CFR3 and prior,	Patched by core rule	Y
CVE-2025-68109	Command injection vulnerability	ChurchCRM is an open-source church management system. In versions prior to 6.5.3, the Database Restore functionality does not validate the content or file extension of uploaded files. As a result, an attacker can upload a web shell file and subsequently upload a .htaccess file to enable direct access to it. Once accessed, the uploaded web shell allows remote code execution (RCE) on the server. Version 6.5.3 fixes the issue.	Patched by core rule	Y
CVE-2024-58294	FreePBX 16 contains an authenticated remote code execution vulnerability	FreePBX 16 contains an authenticated remote code execution vulnerability in the API module that allows attackers with valid session credentials to execute arbitrary commands. Attackers can exploit the 'generatedocs' endpoint by crafting malicious POST	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		requests with bash command injection to establish remote shell access.		
CVE-2025-13481	IBM Aspera Orchestrator 4.0.0 through 4.1.0 could allow an authenticated user to execute arbitrary code	IBM Aspera Orchestrator 4.0.0 through 4.1.0 could allow an authenticated user to execute arbitrary commands with elevated privileges on the system due to improper validation of user supplied input.	Patched by core rule	Y
CVE-2025-64671	Improper neutralization of special elements used in a command ('command injection') in Copilot	Improper neutralization of special elements used in a command ('command injection') in Copilot allows an unauthorized attacker to execute code locally.	Patched by core rule	Y
CVE-2025-64153	A improper neutralization of special elements used in an os command ('os command injection')	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiExtender 7.6.0 through 7.6.3, FortiExtender 7.4.0 through 7.4.7, FortiExtender 7.2 all versions, FortiExtender 7.0 all versions may allow an authenticated attacker to execute unauthorized code or commands via a specific HTTP request.	Patched by core rule	Y
CVE-2025-54100	Improper neutralization of special elements used in a command ('command injection')	Improper neutralization of special elements used in a command ('command injection') in Windows PowerShell allows an unauthorized attacker to execute code locally.	Patched by core rule	Y
CVE-2025-53949	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.2, FortiSandbox 4.4.0 through 4.4.7, FortiSandbox 4.2 all versions, FortiSandbox 4.0 all versions may allow an authenticated attacker to execute unauthorized code on the underlying system via crafted HTTP requests.	Patched by core rule	Y
CVE-2025-40937	Command injection vulnerability	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V4.0.1). The affected application do not properly validate input parameters in its REST API, resulting in improper handling of unexpected arguments. This could allow an authenticated attacker to execute arbitrary code with limited privileges.	Patched by core rule	Y
CVE-2024-56837	Command injection vulnerability	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). Due to the insufficient validation during the installation and load of certain configuration files of the affected device, an attacker could spawn a reverse shell and gain root access on the affected system.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-56836	Command injection vulnerability	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). During the Dynamic DNS configuration of the affected product it is possible to inject additional configuration parameters. Under certain circumstances, an attacker could leverage this vulnerability to spawn a reverse shell and gain root access on the affected system.	Patched by core rule	Y
CVE-2025-14092	Command injection vulnerability	A security vulnerability has been detected in Edimax BR-6478AC V3 1.0.15. This issue affects the function sub_416898 of the file /boafrm/formDebugDiagnosticRun. The manipulation of the argument host leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-14090	Command injection vulnerability	A security flaw has been discovered in AMTT Hotel Broadband Operation System 1.0. This affects an unknown part of the file /manager/card/cardmake_down.php. Performing manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-66404	Command injection vulnerability	MCP Server Kubernetes is an MCP Server that can connect to a Kubernetes cluster and manage it. Prior to 2.9.8, there is a security issue exists in the exec_in_pod tool of the mcp-server-kubernetes MCP Server. The tool accepts user-provided commands in both array and string formats. When a string format is provided, it is passed directly to shell interpretation (sh -c) without input validation, allowing shell metacharacters to be interpreted. This vulnerability can be exploited through direct com	Patched by core rule	Y
CVE-2025-66399	Command injection vulnerability in the operating system	Cacti is an open source performance and fault management framework. Prior to 1.2.29, there is an input-validation flaw in the SNMP device configuration functionality. An authenticated Cacti user can supply crafted SNMP community strings containing control characters (including newlines) that are accepted,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		stored verbatim in the database, and later embedded into backend SNMP operations. In environments where downstream SNMP tooling or wrappers interpret newline-separated tokens as command boundar		
CVE-2025-11787	Command injection vulnerability in the operating system	Command injection vulnerability in the operating system in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2 through the 'GetDNS()', 'CheckPing()' and 'TraceRoute()' functions.	Patched by core rule	Y
CVE-2025-66263	Unauthenticated Arbitrary File Read via Null Byte Injection	Unauthenticated Arbitrary File Read via Null Byte Injection in DB Electronica Telecomunicazioni S.p.A. Mozart FM Transmitter versions 30, 50, 100, 300, 500, 1000, 2000, 3000, 3500, 6000, 7000 allows an attacker to perform Null byte injection in download_setting.php allows reading arbitrary files. The `/var/tdf/download_setting.php` endpoint constructs file paths by concatenating user-controlled `$_GET['filename']` with a forced `.tgz` extension. Running on PHP 5.3.2 (pre-5.3.4), the application	Patched by core rule	Y

Code Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-15078	A vulnerability was detected in itsourcecode Student Management System 1.0.	A vulnerability was detected in itsourcecode Student Management System 1.0. The impacted element is an unknown function of the file /list_report.php. The manipulation of the argument sy results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-15077	A security vulnerability has been detected in itsourcecode Student Management System 1.0.	A security vulnerability has been detected in itsourcecode Student Management System 1.0. The affected element is an unknown function of the file /form137.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-15075	A security flaw has been discovered in itsourcecode Student Management System 1.0.	A security flaw has been discovered in itsourcecode Student Management System 1.0. This issue affects some unknown processing of the file /student_p.php. Performing manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-15074	A vulnerability was identified in itsourcecode Online Frozen Foods Ordering System 1.0.	A vulnerability was identified in itsourcecode Online Frozen Foods Ordering System 1.0. This vulnerability affects unknown code of the file /customer_details.php. Such manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-15073	A vulnerability was determined in itsourcecode Online Frozen Foods Ordering System 1.0.	A vulnerability was determined in itsourcecode Online Frozen Foods Ordering System 1.0. This affects an unknown part of the file /contact_us.php. This manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument Name causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.		
CVE-2025-15053	A flaw has been found in code-projects Student Information System 1.0.	A flaw has been found in code-projects Student Information System 1.0. This issue affects some unknown processing of the file /searchresults.php. Executing manipulation of the argument searchbox can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-15049	A vulnerability was identified in code-projects Online Farm System 1.0.	A vulnerability was identified in code-projects Online Farm System 1.0. Affected is an unknown function of the file /addProduct.php. The manipulation of the argument Username leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-15048	A vulnerability was determined in Tenda WH450 1.0.0.18.	A vulnerability was determined in Tenda WH450 1.0.0.18. This impacts an unknown function of the file /goform/CheckTools of the component HTTP Request Handler. Executing manipulation of the argument ipaddress can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2021-47736	CMSimple_XH 1.7.4 contains an authenticated remote code execution vulnerability	CMSimple_XH 1.7.4 contains an authenticated remote code execution vulnerability in the content editing functionality that allows administrative users to upload malicious PHP files. Attackers with valid credentials can exploit the CSRF token mechanism to create a PHP shell file that enables arbitrary command execution on the server.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-15034	A security flaw has been discovered in itsourcecode Student Management System 1.0.	A security flaw has been discovered in itsourcecode Student Management System 1.0. This affects an unknown part of the file /record.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2024-27708	Iframe injection	Iframe injection vulnerability in airc.pt/solucoes-servicos.solucoes MyNET v.26.06 and before allows a remote attacker to execute arbitrary code via the src parameter.	Patched by core rule	Y
CVE-2025-15014	A security flaw has been discovered in loganhong php loganSite up	A security flaw has been discovered in loganhong php loganSite up to c035fb5c3edd0b2a5e32fd4051cbbc9e61a31426. This affects an unknown function of the file /includes/article_detail.php of the component Article Handler. Performing manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available.	Patched by core rule	Y
CVE-2025-15012	A vulnerability was determined in code-projects Refugee Food Management System 1.0.	A vulnerability was determined in code-projects Refugee Food Management System 1.0. The affected element is an unknown function of the file /home/home.php. This manipulation of the argument a causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-15011	A vulnerability was found in code-projects Simple Stock System 1.0.	A vulnerability was found in code-projects Simple Stock System 1.0. Impacted is an unknown function of the file /logout.php. The manipulation of the argument uname results in sql injection. The attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		can be executed remotely. The exploit has been made public and could be used.		
CVE-2025-15004	A vulnerability was identified in DedeCMS up to 5.7.118.	A vulnerability was identified in DedeCMS up to 5.7.118. This impacts an unknown function of the file /freelist_main.php. The manipulation of the argument orderby leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-15003	A vulnerability was found in SeaCMS up to 13.3.	A vulnerability was found in SeaCMS up to 13.3. The impacted element is an unknown function of the file admin_video.php. Performing manipulation of the argument e_id results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-15002	A vulnerability has been found in SeaCMS up to 13.3.	A vulnerability has been found in SeaCMS up to 13.3. The affected element is an unknown function of the file js/player/dmplayer/dmku/class/mysqli.class.php. Such manipulation of the argument page/limit leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-14990	A security flaw has been discovered in Campcodes Complete Online Beauty Parlor Management System 1.0	A security flaw has been discovered in Campcodes Complete Online Beauty Parlor Management System 1.0. Impacted is an unknown function of the file /admin/view-appointment.php. Performing manipulation of the argument viewid results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-14989	A vulnerability was identified in Campcodes Complete Online Beauty Parlor Management System 1.0.	A vulnerability was identified in Campcodes Complete Online Beauty Parlor Management System 1.0. This issue affects some unknown processing of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/search-invoices.php. Such manipulation leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.		
CVE-2025-14968	A security flaw has been discovered in code-projects Simple Stock System 1.0.	A security flaw has been discovered in code-projects Simple Stock System 1.0. Affected by this issue is some unknown functionality of the file /market/update.php. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-14967	A vulnerability was identified in itsourcecode Student Management System 1.0.	A vulnerability was identified in itsourcecode Student Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /candidates_report.php. The manipulation of the argument school_year leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-14961	A vulnerability was detected in code-projects Simple Blood Donor Management System 1.0.	A vulnerability was detected in code-projects Simple Blood Donor Management System 1.0. The affected element is an unknown function of the file /editedcampaign.php. The manipulation of the argument campaignname results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-14952	A vulnerability was detected in Campcodes Supplier Management System 1.0.	A vulnerability was detected in Campcodes Supplier Management System 1.0. This affects an unknown function of the file /admin/add_category.php. Performing manipulation of the argument txtCategoryName results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		used.		
CVE-2025-14950	A weakness has been identified in code-projects Scholars Tracking System 1.0. T	A weakness has been identified in code-projects Scholars Tracking System 1.0. The affected element is an unknown function of the file /delete_post.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-14940	A vulnerability was determined in code-projects Scholars Tracking System 1.0.	A vulnerability was determined in code-projects Scholars Tracking System 1.0. The affected element is an unknown function of the file /admin/delete_user.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-14939	A vulnerability was found in code-projects Online Appointment Booking System 1.0.	A vulnerability was found in code-projects Online Appointment Booking System 1.0. Impacted is an unknown function of the file /admin/deletemanager.php. The manipulation of the argument managername results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-67843	A Server-Side Template Injection (SSTI)	A Server-Side Template Injection (SSTI) vulnerability in the MDX Rendering Engine in Mintlify Platform before 2025-11-15 allows remote attackers to execute arbitrary code via inline JSX expressions in an MDX file.	Patched by core rule	Y
CVE-2025-14900	A security vulnerability has been detected in CodeAstro Real Estate Management System 1.0.	A security vulnerability has been detected in CodeAstro Real Estate Management System 1.0. Affected is an unknown function of the file /admin/userdelete.php of the component Administrator Endpoint.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.		
CVE-2025-14899	A weakness has been identified in CodeAstro Real Estate Management System 1.0.	A weakness has been identified in CodeAstro Real Estate Management System 1.0. This impacts an unknown function of the file /admin/stateadd.php of the component Administrator Endpoint. This manipulation causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-14898	A security flaw has been discovered in CodeAstro Real Estate Management System 1.0.	A security flaw has been discovered in CodeAstro Real Estate Management System 1.0. This affects an unknown function of the file /admin/userbuilderdelete.php of the component Administrator Endpoint. The manipulation results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-14897	A vulnerability was identified in CodeAstro Real Estate Management System 1.0.	A vulnerability was identified in CodeAstro Real Estate Management System 1.0. The impacted element is an unknown function of the file /admin/useragentdelete.php of the component Administrator Endpoint. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-14884	A vulnerability was detected in D-Link DIR-605 202WWB03.	A vulnerability was detected in D-Link DIR-605 202WWB03. Affected by this issue is some unknown functionality of the component Firmware Update Service. Performing manipulation results in command injection. The attack can be initiated remotely. The exploit is now public and may be used. This vulnerability only affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		products that are no longer supported by the maintainer.		
CVE-2025-14877	A vulnerability was identified in Campcodes Supplier Management System 1.0. This affects an unknown	A vulnerability was identified in Campcodes Supplier Management System 1.0. This affects an unknown function of the file /admin/add_retailer.php. The manipulation of the argument cmbAreaCode leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-14856	A security vulnerability has been detected in y_project RuoYi up to 4.8.1. The affected element is a	A security vulnerability has been detected in y_project RuoYi up to 4.8.1. The affected element is an unknown function of the file /monitor/cache/getnames. Such manipulation of the argument fragment leads to code injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-14837	A vulnerability has been found in ZZCMS 2025. Affected by this issue is the function stripfxg of the	A vulnerability has been found in ZZCMS 2025. Affected by this issue is the function stripfxg of the file /admin/siteconfig.php of the component Backend Website Settings Module. Such manipulation of the argument icp leads to code injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-14834	A weakness has been identified in code-projects Simple Stock System 1.0. This affects an unknown fun	A weakness has been identified in code-projects Simple Stock System 1.0. This affects an unknown function of the file /checkuser.php. Executing manipulation of the argument Username can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2023-53929	phpMyFAQ 3.1.12 contains a CSV injection vulnerability that allows authenticated users to inject mal	phpMyFAQ 3.1.12 contains a CSV injection vulnerability that allows authenticated users to inject malicious formulas	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		into their profile names. Attackers can modify their user profile name with a payload like 'calc|a!z|' to trigger code execution when an administrator exports user data as a CSV file.		
CVE-2023-53905	ProjectSend r1605 contains a CSV injection vulnerability that allows authenticated user	ProjectSend r1605 contains a CSV injection vulnerability that allows authenticated users to inject malicious formulas into user profile names. Attackers can craft payloads like =calc|a!z| in the name field to trigger code execution when administrators export action logs as CSV files.	Patched by core rule	Y
CVE-2025-14730	A security flaw has been discovered in CTCMS Content Management System up to 2.1.2.	A security flaw has been discovered in CTCMS Content Management System up to 2.1.2. The impacted element is an unknown function in the library /ctcms/libs/Ct_Config.php of the component Backend System Configuration Module. The manipulation of the argument Cj_Add/Cj_Edit results in code injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-14729	A vulnerability was identified in CTCMS Content Management System up to 2.1.2. The affected element	A vulnerability was identified in CTCMS Content Management System up to 2.1.2. The affected element is the function Save of the file /ctcms/libs/Ct_App.php of the component Backend App Configuration Module. The manipulation of the argument CT_App_Paytype leads to code injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-66434	An SSTI (Server-Side Template Injection) vulnerability exists in the get_dunning_letter_text method	An SSTI (Server-Side Template Injection) vulnerability exists in the get_dunning_letter_text method of Frappe ERPNext through 15.89.0. The function renders attacker-controlled Jinja2 templates (body_text) using frappe.render_template()	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with a user-supplied context (doc). Although Frappe uses a custom SandboxedEnvironment, several dangerous globals such as frappe.db.sql are still available in the execution context via get_safe_globals(). An authenticated attacker with access to configure Dunning		
CVE-2025-14711	A flaw has been found in FantasticLBP Hotels Server	A flaw has been found in FantasticLBP Hotels Server up to 67b44df162fab26df209bd5d5d542875fcbec1d0. This vulnerability affects unknown code of the file /controller/api/hotelList.php. This manipulation of the argument pickedHotelName/type causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery The vendor was contacted early about this disclosure but did n	Patched by core rule	Y
CVE-2025-14710	A vulnerability was detected in FantasticLBP Hotels Server	A vulnerability was detected in FantasticLBP Hotels Server up to 67b44df162fab26df209bd5d5d542875fcbec1d0. This affects an unknown part of the file /controller/api/OrderList.php. The manipulation of the argument telephone results in sql injection. The attack can be executed remotely. The exploit is now public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted ea	Patched by core rule	Y
CVE-2025-14668	A vulnerability was detected in campcodes Advanced Online Examination System 1.0.	A vulnerability was detected in campcodes Advanced Online Examination System 1.0. This affects an unknown function of the file /query/loginExe.php. Performing manipulation of the argument Username	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.		
CVE-2025-14667	A security vulnerability has been detected in itsourcecode COVID Tracking System 1.0.	A security vulnerability has been detected in itsourcecode COVID Tracking System 1.0. The impacted element is an unknown function of the file /admin/?page=system_info. Such manipulation of the argument meta_value leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-14666	A weakness has been identified in itsourcecode COVID Tracking System 1.0.	A weakness has been identified in itsourcecode COVID Tracking System 1.0. The affected element is an unknown function of the file /admin/?page=user. This manipulation of the argument Username causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-14659	A vulnerability was detected in D-Link DIR-860LB1 and DIR-868LB1 203b01/203b03.	A vulnerability was detected in D-Link DIR-860LB1 and DIR-868LB1 203b01/203b03. Affected is an unknown function of the component DHCP Daemon. The manipulation of the argument Hostname results in command injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-14648	A security vulnerability has been detected in DedeBIZ up to 6.5.9.	A security vulnerability has been detected in DedeBIZ up to 6.5.9. Affected by this vulnerability is an unknown functionality of the file /src/admin/catalog_add.php. Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-14647	A weakness has been identified in code-projects Computer Book Store 1.0.	A weakness has been identified in code-projects Computer Book Store 1.0. Affected is an unknown function of the file /admin_delete.php. This manipulation of the argument bookisbn causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-14589	A weakness has been identified in code-projects Prison Management System 2.0.	A weakness has been identified in code-projects Prison Management System 2.0. This issue affects some unknown processing of the file /admin/search.php. Executing manipulation of the argument keyname can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-14578	A weakness has been identified in itsourcecode Student Management System 1.0.	A weakness has been identified in itsourcecode Student Management System 1.0. The affected element is an unknown function of the file /update_account.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-14571	A vulnerability has been found in projectworlds Advanced Library Management System 1.0.	A vulnerability has been found in projectworlds Advanced Library Management System 1.0. Affected by this issue is some unknown functionality of the file /borrow_book.php. Such manipulation of the argument roll_number leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-14570	A flaw has been found in projectworlds Advanced Library Management System 1.0.	A flaw has been found in projectworlds Advanced Library Management System 1.0. Affected by this vulnerability is an unknown functionality of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the file /view_admin.php. This manipulation of the argument admin_id causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.		
CVE-2025-14566	A security flaw has been discovered in kidaze CourseSelectionSystem	A security flaw has been discovered in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. The impacted element is an unknown function of the file /Profilers/SProfile/reg.php. Performing manipulation of the argument USN results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-14565	A vulnerability was identified in kidaze CourseSelectionSystem	A vulnerability was identified in kidaze CourseSelectionSystem up to 42cd892b40a18d50bd4ed1905fa89f939173a464. The affected element is an unknown function of the file /Profilers/SProfile/login1.php. Such manipulation of the argument Username leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-13780	pgAdmin versions up to 9.10 are affected by a Remote Code Execution (RCE) vulnerability that occurs	pgAdmin versions up to 9.10 are affected by a Remote Code Execution (RCE) vulnerability that occurs when running in server mode and performing restores from PLAIN-format dump files. This issue allows attackers to inject and execute arbitrary commands on the server hosting pgAdmin, posing a critical risk to the integrity and security of the database management system and underlying data.	Patched by core rule	Y
CVE-2025-66474	XWiki Rendering is a generic rendering system that converts textual input in a given syntax	XWiki Rendering is a generic rendering system that converts textual input in a given syntax (wiki syntax, HTML, etc) into	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		another syntax (XHTML, etc). Versions 16.10.9 and below, 17.0.0-rc-1 through 17.4.2 and 17.5.0-rc-1 through 17.5.0 have insufficient protection against {{/html}} injection, which attackers can exploit through RCE. Any user who can edit their own profile or any other document can execute arbitrary script macros, including Groovy and Python macros, which enable remote code exec		
CVE-2024-56840	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0).	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). Under certain conditions, IPsec may allow code injection in the affected device. An attacker could leverage this scenario to execute arbitrary code as root user.	Patched by core rule	Y
CVE-2024-56839	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0).	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). Code injection can be achieved when the affected device is using VRF (Virtual Routing and Forwarding). An attacker could leverage this scenario to execute arbitrary code as root user.	Patched by core rule	Y
CVE-2024-56838	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0).	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). The SCEP client available in the affected device for secure certificate enrollment lacks validation of multiple fields. An attacker could leverage this scenario to execute arbitrary code as root user.	Patched by core rule	Y
CVE-2024-56835	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0).	A vulnerability has been identified in RUGGEDCOM ROX II family (All versions < V2.17.0). The DHCP Server configuration file of the affected products is subject to code injection. An attacker could leverage this vulnerability to spawn a reverse shell and gain root access on the affected system.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-14230	A vulnerability was detected in code-projects Daily Time Recording System 4.5.0.	A vulnerability was detected in code-projects Daily Time Recording System 4.5.0. The impacted element is an unknown function of the file /admin/add_payroll.php. Performing manipulation of the argument detail_Id results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-14229	A security vulnerability has been detected in SourceCodester Inventory Management System 1.0.	A security vulnerability has been detected in SourceCodester Inventory Management System 1.0. The affected element is an unknown function of the component SVC Report Export. Such manipulation leads to csv 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-2025-14225	A vulnerability was determined in D-Link DCS-930L 1.15.04.	A vulnerability was determined in D-Link DCS-930L 1.15.04. This affects an unknown part of the file /setSystemAdmin of the component alphapd. Executing manipulation of the argument AdminID can lead to command injection. The attack can be executed 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-2025-14222	A flaw has been found in code-projects Employee Profile Management System 1.0.	A flaw has been found in code-projects Employee Profile Management System 1.0. Affected is an unknown function of the file /print_personnel_report.php. This manipulation of the argument per_id causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-14214	A vulnerability has been found in itsourcecode Student Information System 1.0.	A vulnerability has been found in itsourcecode Student Information System 1.0. This affects an unknown part of the file /section_edit1.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.		
CVE-2025-14203	A flaw has been found in code-projects Question Paper Generator up to 1.0.	A flaw has been found in code-projects Question Paper Generator up to 1.0. This vulnerability affects unknown code of the file /selectquestionuser.php. This manipulation of the argument subid causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-14193	A vulnerability was determined in code-projects Employee Profile Management System 1.0.	A vulnerability was determined in code-projects Employee Profile Management System 1.0. This vulnerability affects unknown code of the file /view_personnel.php. Executing manipulation of the argument per_id can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-14012	A vulnerability was determined in JIZHICMS up to 2.5.5.	A vulnerability was determined in JIZHICMS up to 2.5.5. The affected element is the function deleteAll/findAll/delete of the file /index.php/admins/Comment/deleteAll.html of the component Batch Delete Comments. Executing manipulation can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-14011	A vulnerability was found in JIZHICMS up to 2.5.5.	A vulnerability was found in JIZHICMS up to 2.5.5. Impacted is the function commentlist of the file /index.php/admins/Comment/addcomment.html of the component Add Display Name Field. Performing manipulation of the argument aid/tid results in sql injection. The attack can be initiated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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-2025-66294	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, a Server-Side Template Injection (SSTI)	Grav is a file-based Web platform. Prior to 1.8.0-beta.27, a Server-Side Template Injection (SSTI) vulnerability exists in Grav that allows authenticated attackers with editor permissions to execute arbitrary commands on the server and, under certain conditions, may also be exploited by unauthenticated attackers. This vulnerability stems from weak regex validation in the cleanDangerousTwig method. This vulnerability is fixed in 1.8.0-beta.27.	Patched by core rule	Y
CVE-2025-13811	A vulnerability was determined in jsnjfz WebStack-Guns 1.0.	A vulnerability was determined in jsnjfz WebStack-Guns 1.0. This vulnerability affects unknown code of the file src/main/java/com/jsnjfz/manage/core/common/constant/factory/PageFactory.java. Executing manipulation of the argument sort can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-68600	Server-Side Request Forgery (SSRF) vulnerability in Yannick Lefebvre Link Library link-library	Server-Side Request Forgery (SSRF) vulnerability in Yannick Lefebvre Link Library link-library allows Server Side Request Forgery.This issue affects Link Library: from n/a through <= 7.8.4.	Patched by core rule	Y
CVE-2025-68500	Server-Side Request Forgery (SSRF) vulnerability	Server-Side Request Forgery (SSRF) vulnerability in bdthemes Prime ddons For Elementor bdthemes-prime-slider-lite allows Server Side Request Forgery.This issue affects Prime Slider Addons For Elementor: from n/a through <= 4.0.10.	Patched by core rule	Y
CVE-2025-67623	Server-Side Request Forgery (SSRF) vulnerability in 6Storage 6Storage	Server-Side Request Forgery (SSRF) vulnerability in 6Storage 6Storage Rentals 6storage-rentals allows Server Side Request Forgery.This issue affects 6Storage Rentals: from n/a through <= 2.19.9.	Patched by core rule	Y
CVE-2025-67743	Local Deep Research is an AI-powered research assistant for deep, iterative research.	Local Deep Research is an AI-powered research assistant for deep, iterative research. In versions from 1.3.0 to before 1.3.9, the download service (download_service.py) makes HTTP requests using raw requests.get() without utilizing the application's SSRF protection (safe_requests.py). This can allow attackers to access internal services and attempt to reach cloud provider metadata endpoints (AWS/GCP/Azure), as well as perform internal network reconnaissance, by submitting malicious URLs through	Patched by core rule	Y
CVE-2025-13999	The HTML5 Audio Player The Ultimate No-Code Podcast, MP3 & Audio Player plugin for WordPress	The HTML5 Audio Player The Ultimate No-Code Podcast, MP3 & Audio Player plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions from 2.4.0 up to, and including, 2.5.1 via the getIcyMetadata() function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		information from internal services.		
CVE-2025-14443	A flaw was found in ose-openshift-apiserver. This vulnerability allows internal network enumeration,	A flaw was found in ose-openshift-apiserver. This vulnerability allows internal network enumeration, service discovery, limited information disclosure, and potential denial-of-service (DoS) through Server-Side Request Forgery (SSRF) due to missing IP address and network-range validation when processing user-supplied image references.	Patched by core rule	Y
CVE-2025-67494	ZITADEL is an open-source identity infrastructure tool.	ZITADEL is an open-source identity infrastructure tool. Versions 4.7.0 and below are vulnerable to an unauthenticated, full-read SSRF vulnerability. The ZITADEL Login UI (V2) treats the x-zitadel-forward-host header as a trusted fallback for all deployments, including self-hosted instances. This allows an unauthenticated attacker to force the server to make HTTP requests to arbitrary domains, such as internal addresses, and read the responses, enabling data exfiltration and bypassing network-seg	Patched by core rule	Y
CVE-2021-47703	OpenBMCS 2.4 contains an unauthenticated SSRF vulnerability that allows attackers to bypass firewall	OpenBMCS 2.4 contains an unauthenticated SSRF vulnerability that allows attackers to bypass firewalls and initiate service and network enumeration on the internal network through the affected application, allowing hijacking of current sessions. Attackers can specify an external domain in the 'ip' parameter to force the application to make an HTTP request to an arbitrary destination host.	Patched by core rule	Y
CVE-2025-65958	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline.	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.6.37, a Server-Side Request Forgery (SSRF) vulnerability in Open WebUI allows any authenticated user to force the server to make HTTP requests to arbitrary URLs. This can be exploited to access cloud metadata endpoints (AWS/GCP/Azure), scan internal networks, access	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		internal services behind firewalls, and exfiltrate sensitive information. No special permissions beyond basic authenticatio		
CVE-2025-14008	A flaw has been found in dayrui XunRuiCMS up to 4.7.1.	A flaw has been found in dayrui XunRuiCMS up to 4.7.1. This vulnerability affects unknown code of the file admin79f2ec220c7e.php?c=api&m=test_site_domain of the component Project Domain Change Test. This manipulation of the argument v causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-66201	LibreChat is a ChatGPT clone with additional features. Prior to version 0.8.1-rc2	LibreChat is a ChatGPT clone with additional features. Prior to version 0.8.1-rc2, LibreChat is vulnerable to Server-side Request Forgery (SSRF), by passing specially crafted OpenAPI specs to its "Actions" feature and making the LLM use those actions. It could be used by an authenticated user with access to this feature to access URLs only accessible to the LibreChat server (such as cloud metadata services, through which impersonation of the server might be possible). This issue has been patched	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-39037	MyNET up to v26.08.316 was discovered to contain an Unauthenticated SQL Injection vulnerability	MyNET up to v26.08.316 was discovered to contain an Unauthenticated SQL Injection vulnerability via the intmenu parameter.	Patched by core rule	Y
CVE-2025-68590	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CRM Perks Integration for Contact Form 7 HubSpot cf7-hubspot allows Blind SQL Injection.This issue affects Integration for Contact Form 7 HubSpot: from n/a through <= 1.4.2.	Patched by core rule	Y
CVE-2025-68570	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in captivateaudio Captivate Sync captivatesync-trade allows Blind SQL Injection.This issue affects Captivate Sync: from n/a through <= 3.2.2.	Patched by core rule	Y
CVE-2025-68519	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BeRocket Brands for WooCommerce brands-for-woocommerce allows Blind SQL Injection.This issue affects Brands for WooCommerce: from n/a through <= 3.8.6.3.	Patched by core rule	Y
CVE-2025-68496	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Syed Balkhi User Feedback userfeedback-lite allows Blind SQL Injection.This issue affects User Feedback: from n/a through <= 1.10.1.	Patched by core rule	Y
CVE-2023-36525	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPJobBoard allows Blind SQL Injection.This issue affects WPJobBoard: from n/a through 5.9.0.	Patched by core rule	Y
CVE-2025-65354	Improper input handling in /Grocery/search_products_itname.php inPuneethReddyHC event-management 1.0	Improper input handling in /Grocery/search_products_itname.php inPuneethReddyHC event-management 1.0 permits SQL injection via the sitem_name POST	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameter. Crafted payloads can alter query logic and disclose database contents. Exploitation may result in sensitive data disclosure and backend compromise.		
CVE-2023-53982	PMB 7.4.6 contains a SQL injection vulnerability in the storage parameter of the ajax.php endpoint	PMB 7.4.6 contains a SQL injection vulnerability in the storage parameter of the ajax.php endpoint that allows remote attackers to manipulate database queries. Attackers can exploit the unsanitized 'id' parameter by injecting conditional sleep statements to extract information or perform time-based blind SQL injection attacks.	Patched by core rule	Y
CVE-2021-47720	Orangescrum 1.8.0 contains an authenticated SQL injection vulnerability	Orangescrum 1.8.0 contains an authenticated SQL injection vulnerability that allows authorized users to manipulate database queries through multiple vulnerable parameters. Attackers can inject malicious SQL code into parameters like old_project_id, project_id, uuid, and uniqid to potentially extract or modify database information.	Patched by core rule	Y
CVE-2024-57521	SQL Injection vulnerability in RuoYi v.4.7.9	SQL Injection vulnerability in RuoYi v.4.7.9 and before allows a remote attacker to execute arbitrary code via the createTable function in SqlUtil.java.	Patched by core rule	Y
CVE-2025-68561	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ruben Garcia AutomatorWP allows SQL Injection.This issue affects AutomatorWP: from n/a through 5.2.4.	Patched by core rule	Y
CVE-2025-68550	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VillaTheme WPBulky allows Blind SQL Injection.This issue affects WPBulky: from n/a through 1.1.13.	Patched by core rule	Y
CVE-2023-53975	Atom CMS 2.0 contains an unauthenticated SQL injection vulnerability	Atom CMS 2.0 contains an unauthenticated SQL injection vulnerability that allows remote attackers to manipulate database queries through unvalidated parameters. Attackers can inject malicious SQL code in the 'id' parameter of the admin index page to execute	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		time-based blind SQL injection attacks.		
CVE-2023-53972	WebTareas 2.4 contains a SQL injection vulnerability in the webTareasSID cookie parameter	WebTareas 2.4 contains a SQL injection vulnerability in the webTareasSID cookie parameter that allows unauthenticated attackers to manipulate database queries. Attackers can exploit error-based and time-based blind SQL injection techniques to extract database information and potentially access sensitive system data.	Patched by core rule	Y
CVE-2025-12514	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Centreon Infra Monitoring - Open-tickets (Notification rules configuration parameters, Open tickets modules) allows SQL Injection to user with elevated privileges.This issue affects Infra Monitoring - Open-tickets: from 24.10.0 before 24.10.5, from 24.04.0 before 24.04.5, from 23.10.0 before 23.10.4.	Patched by core rule	Y
CVE-2025-46268	Advantech WebAccess/SCADA is vulnerable to SQL injection	Advantech WebAccess/SCADA is vulnerable to SQL injection, which may allow an attacker to execute arbitrary SQL commands.	Patched by core rule	Y
CVE-2025-68400	ChurchCRM is an open-source church management system. A SQL Injection vulnerability	ChurchCRM is an open-source church management system. A SQL Injection vulnerability exists in the legacy endpoint `/Reports/ConfirmReportEmail.php` in ChurchCRM prior to version 6.5.3. Although the feature was removed from the UI, the file remains deployed and reachable directly via URL. This is a classic case of *dead but reachable code*. Any authenticated user - including one with zero assigned permissions - can exploit SQL injection through the `familyId` parameter. Version 6.5.3 fixes the is	Patched by core rule	Y
CVE-2025-68112	ChurchCRM is an open-source church management system. In versions prior to 6.5.3, a SQL injection vulnerability.	ChurchCRM is an open-source church management system. In versions prior to 6.5.3, a SQL injection vulnerability in ChurchCRM's Event Attendee Editor allows authenticated users to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execute arbitrary SQL commands, leading to complete database compromise, administrative credential theft, and potential system takeover. The vulnerability enables attackers to extract sensitive member data, authentication credentials, and financial information from the church management system. Version 6.5.3 contains a		
CVE-2025-67877	ChurchCRM is an open-source church management system. Versions prior to 6.5.3 have a SQL injection vulnerability	ChurchCRM is an open-source church management system. Versions prior to 6.5.3 have a SQL injection vulnerability in the `src/CartToFamily.php` file, specifically in how the `PersonAddress` POST parameter is handled. Unlike other parameters in the same file which are correctly cast to integers using the `InputUtils` class, the `PersonAddress` parameter is missing the type definition. This allows an attacker to inject arbitrary SQL commands directly into the query. Version 6.5.3 fixes the issue.	Patched by core rule	Y
CVE-2025-67736	The FreePBX module tts (Text to Speech) for FreePBX, an open-source web-based graphical user interfa (GUI) that manages Asterisk.	The FreePBX module tts (Text to Speech) for FreePBX, an open-source web-based graphical user interface (GUI) that manages Asterisk. Versions prior to 16.0.5 and 17.0.5 are vulnerable to SQL injection by authenticated users with administrator access. Authenticated users with administrative access to the Administrator Control Panel (ACP) can leverage this SQL injection vulnerability to extract sensitive information from the database and execute code on the system as the `asterisk` user with chaine	Patched by core rule	Y
CVE-2025-14383	The Booking Calendar plugin for WordPress is vulnerable to time-based blind SQL Injection	The Booking Calendar plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'dates_to_check' parameter in all versions up to, and including, 10.14.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.		
CVE-2025-13126	The wpForo Forum plugin for WordPress is vulnerable to generic SQL Injection	The wpForo Forum plugin for WordPress is vulnerable to generic SQL Injection via the `post_args` and `topic_args` parameters in all versions up to, and including, 2.4.12 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-13089	The WP Directory Kit plugin for WordPress is vulnerable to SQL Injection via the 'hide_fields' and the 'attr_search' parameter in all versions up to, and including, 1.4.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query	The WP Directory Kit plugin for WordPress is vulnerable to SQL Injection via the 'hide_fields' and the 'attr_search' parameter in all versions up to, and including, 1.4.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-13077	The payamito sms woocommerce plugin for WordPress is vulnerable to time-based blind SQL	The payamito sms woocommerce plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'columns' parameter in all versions up to, and including, 1.3.5. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive infor	Patched by core rule	Y
CVE-2025-14169	The FunnelKit - Funnel Builder for WooCommerce Checkout plugin for WordPress is vulnerable to time- based	The FunnelKit - Funnel Builder for WooCommerce Checkout plugin for WordPress is vulnerable to time-based blind SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	blind SQLi.	Injection via the 'opid' parameter in all versions up to, and including, 3.13.1.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the databa		
CVE-2025-14068	The WPNakama plugin for WordPress is vulnerable to time-based SQL Injection	The WPNakama plugin for WordPress is vulnerable to time-based SQL Injection via the 'order_by' parameter in all versions up to, and including, 0.6.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2024-58307	CSZCMS 1.3.0 contains an authenticated SQL injection vulnerability in the members view functionality	CSZCMS 1.3.0 contains an authenticated SQL injection vulnerability in the members view functionality that allows authenticated attackers to manipulate database queries. Attackers can inject malicious SQL code through the view parameter to potentially execute time-based blind SQL injection attacks and extract database information.	Patched by core rule	Y
CVE-2025-13214	IBM Aspera Orchestrator 4.0.0 through 4.1.0 is vulnerable to SQL injection.	IBM Aspera Orchestrator 4.0.0 through 4.1.0 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL s tatements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	Patched by core rule	Y
CVE-2025-65950	WBCE CMS is a content management system. In versions 1.6.4 and below, the user management module allows a low-privileged authenticated user with permissions to modify users to execute arbitrary SQL queries.	WBCE CMS is a content management system. In versions 1.6.4 and below, the user management module allows a low-privileged authenticated user with permissions to modify users to execute arbitrary SQL queries. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		can be escalated to a full database compromise, data exfiltration, effectively bypassing all security controls. The vulnerability exists in the admin/users/save.php script, which handles updates to user profiles. The script improperly processes the groups[] parameter sent from the user e		
CVE-2025-67501	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users.	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. Versions 3.5.4 and below contain an SQL Injection vulnerability in the /html/matPat/editar_categoria.php endpoint. The application fails to properly validate and sanitize user inputs in the id_categoria parameter, which allows attackers to inject malicious SQL payloads for direct execution. This issue is fixed in version 3.5.5.	Patched by core rule	Y
CVE-2025-66313	ChurchCRM is an open-source church management system.	ChurchCRM is an open-source church management system. In ChurchCRM 6.2.0 and earlier, there is a time-based blind SQL injection in the handling of the 1FieldSec parameter. Injecting SLEEP() causes deterministic server-side delays, proving the value is incorporated into a SQL query without proper parameterization. The issue allows data exfiltration and modification via blind techniques.	Patched by core rule	Y
CVE-2025-63535	A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the abs.php component.	A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the abs.php component. The application fails to properly sanitize usersupplied input in SQL queries, allowing an attacker to inject arbitrary SQL code. By manipulating the search field, an attacker can bypass authentication and gain unauthorized access to the system.	Patched by core rule	Y
CVE-2025-63532	A SQL injection vulnerability exists in the Blood Bank Management System 1.0	A SQL injection vulnerability exists in the Blood Bank Management System 1.0 within the cancel.php component. The application fails to properly sanitize user-supplied input in SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		queries, allowing an attacker to inject arbitrary SQL code. By manipulating the search field, an attacker can bypass authentication and gain unauthorized access to the system.		
CVE-2025-13757	SQL Injection vulnerability in last usage logs in Devolutions Server.	SQL Injection vulnerability in last usage logs in Devolutions Server.This issue affects Devolutions Server: through 2025.2.20, through 2025.3.8.	Patched by core rule	Y
CVE-2025-11461	Multiple SQL Injections in Frappe CRM Dashboard Controller due to unsafe concatenation of user-controlled parameters into dynamic SQL statements.	Multiple SQL Injections in Frappe CRM Dashboard Controller due to unsafe concatenation of user-controlled parameters into dynamic SQL statements. This issue affects Frappe CRM: 1.53.1.	Patched by core rule	Y

Security Misconfiguration Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-53892	Blackcat CMS 1.4 contains a remote code execution vulnerability	Blackcat CMS 1.4 contains a remote code execution vulnerability that allows authenticated administrators to upload malicious PHP files through the jquery plugin manager. Attackers can upload a zip file with a PHP shell script and execute arbitrary system commands by accessing the uploaded plugin's PHP file with a 'code' parameter.	Patched by core rule	Y
CVE-2023-53889	Perch CMS 3.2 contains a remote code execution vulnerability	Perch CMS 3.2 contains a remote code execution vulnerability that allows authenticated administrators to upload arbitrary PHP files through the assets management interface. Attackers can upload a malicious .phar file with embedded system command execution capabilities to execute arbitrary commands on the server.	Patched by core rule	NA
CVE-2023-53868	Coppermine Gallery 1.6.25 contains a remote code execution vulnerability	Coppermine Gallery 1.6.25 contains a remote code execution vulnerability that allows authenticated attackers to upload malicious PHP files through the plugin manager. Attackers can upload a zipped PHP file with system commands to the plugin directory and execute arbitrary code by accessing the uploaded plugin script.	Patched by core rule	Y
CVE-2025-34506	WBCE CMS version 1.6.3 and prior contains an authenticated remote code execution vulnerability	WBCE CMS version 1.6.3 and prior contains an authenticated remote code execution vulnerability that allows administrators to upload malicious modules. Attackers can craft a specially designed ZIP module with embedded PHP reverse shell code to gain remote system access when the module is installed.	Patched by core rule	Y
CVE-2024-58313	xbtitFM 4.1.18 contains an insecure file upload vulnerability	xbtitFM 4.1.18 contains an insecure file upload vulnerability that allows authenticated attackers with administrative privileges to upload and execute arbitrary PHP code through the file_hosting feature. Attackers can bypass file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		type restrictions by modifying the Content-Type header to image/gif, adding GIF89a magic bytes, and using alternate PHP tags to upload web shells that execute system commands.		
CVE-2025-65471	An arbitrary file upload vulnerability in the /admin/manager.php component of EasyImages 2.0 v2.8.6	An arbitrary file upload vulnerability in the /admin/manager.php component of EasyImages 2.0 v2.8.6 and below allows attackers to execute arbitrary code via uploading a crafted PHP file.	Patched by core rule	Y
CVE-2024-58283	WBCE CMS version 1.6.2 contains a remote code execution vulnerability	WBCE CMS version 1.6.2 contains a remote code execution vulnerability that allows authenticated attackers to upload malicious PHP files through the Elfinder file manager. Attackers can exploit the file upload functionality in the elfinder connector to upload a web shell and execute arbitrary system commands through a user-controlled parameter.	Patched by core rule	Y
CVE-2024-58282	Serendipity 2.5.0 contains a remote code execution vulnerability	Serendipity 2.5.0 contains a remote code execution vulnerability that allows authenticated administrators to upload malicious PHP files through the media upload functionality. Attackers can exploit the file upload mechanism by creating a PHP shell with a command execution form that enables arbitrary system command execution on the web server.	Patched by core rule	Y
CVE-2024-58281	Dotclear 2.29 contains a remote code execution vulnerability	Dotclear 2.29 contains a remote code execution vulnerability that allows authenticated attackers to upload malicious PHP files through the media upload functionality. Attackers can exploit the file upload process by crafting a PHP shell with a command execution form to gain system access through the uploaded file.	Patched by core rule	Y
CVE-2024-58279	appRain CMF 4.0.5 contains an authenticated remote code execution vulnerability	appRain CMF 4.0.5 contains an authenticated remote code execution vulnerability that allows administrative users to upload malicious PHP files through the filemanager upload endpoint. Attackers can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leverage authenticated access to generate a web shell with command execution capabilities by uploading a crafted PHP file to the site's uploads directory.		
CVE-2025-56704	LeptonCMS version 7.3.0 contains an arbitrary file upload vulnerability	LeptonCMS version 7.3.0 contains an arbitrary file upload vulnerability, which is caused by the lack of proper validation for uploaded files. An authenticated attacker can exploit this vulnerability by uploading a specially crafted ZIP/PHP file to execute arbitrary code.	Patched by core rule	NA

Broken Access Control Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-15050	A security vulnerability has been detected in code-projects Student File Management System 1.0.	A security vulnerability has been detected in code-projects Student File Management System 1.0. This affects an unknown part of the file /save_file.php. Such manipulation of the argument File leads to unrestricted upload. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-15009	A flaw has been found in liweiyi ChestnutCMS up to 1.5.8.	A flaw has been found in liweiyi ChestnutCMS up to 1.5.8. This vulnerability affects the function FilenameUtils.getExtension of the file /dev-api/common/upload of the component Filename Handler. Executing manipulation of the argument File can lead to unrestricted upload. The attack may be launched remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-14885	A flaw has been found in SourceCodester Client Database Management System 1.0.	A flaw has been found in SourceCodester Client Database Management System 1.0. This affects an unknown part of the file /user_leads.php of the component Leads Generation Module. Executing manipulation can lead to unrestricted upload. The attack can be launched remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-14642	A vulnerability has been found in code-projects Computer Laboratory System 1.0.	A vulnerability has been found in code-projects Computer Laboratory System 1.0. Impacted is an unknown function of the file technical_staff_pic.php. Such manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-14641	A flaw has been found in code-projects Computer Laboratory System 1.0.	A flaw has been found in code-projects Computer Laboratory System 1.0. This issue affects some unknown processing of the file admin/admin_pic.php. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument image causes unrestricted upload. The attack may be initiated remotely. The exploit has been published and may be used.		
CVE-2025-14582	A vulnerability was detected in campcodes Online Student Enrollment System 1.0.	A vulnerability was detected in campcodes Online Student Enrollment System 1.0. This affects an unknown function of the file /admin/index.php?page=user-profile. Performing manipulation of the argument userphoto results in unrestricted upload. The attack can be initiated remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-14530	A vulnerability has been found in SourceCodester Real Estate Property Listing App 1.0.	A vulnerability has been found in SourceCodester Real Estate Property Listing App 1.0. The impacted element is an unknown function of the file /admin/property.php. Such manipulation of the argument image leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-14219	A weakness has been identified in Campcodes Retro Basketball Shoes Online Store 1.0.	A weakness has been identified in Campcodes Retro Basketball Shoes Online Store 1.0. The impacted element is an unknown function of the file /admin/admin_running.php. Executing manipulation of the argument product_image can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-14195	A security flaw has been discovered in code-projects Employee Profile Management System 1.0.	A security flaw has been discovered in code-projects Employee Profile Management System 1.0. Impacted is an unknown function of the file /profiling/add_file_query.php. The manipulation of the argument per_file results in unrestricted upload. The attack may be launched remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-2406	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Verisay Communication and Information Technology Industry and Trade Ltd. Co. Trizbi allows Cross-Site Scripting (XSS).This issue affects Trizbi: before 2.144.4.	Patched by core rule	Y
CVE-2025-2405	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Verisay Communication and Information Technology Industry and Trade Ltd. Co. Titarus allows Cross-Site Scripting (XSS).This issue affects Titarus: before 2.144.4.	Patched by core rule	Y
CVE-2025-2307	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Verisay Communication and Information Technology Industry and Trade Ltd. Co. Aidango allows Cross-Site Scripting (XSS).This issue affects Aidango: before 2.144.4.	Patched by core rule	Y
CVE-2024-40317	A reflected cross-site scripting (XSS) vulnerability in MyNET up to v26.08	A reflected cross-site scripting (XSS) vulnerability in MyNET up to v26.08 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload into the parameter HTTP.	Patched by core rule	Y
CVE-2024-35322	MyNET up to v26.08 was discovered to contain a reflected cross-site scripting (XSS) vulnerability	MyNET up to v26.08 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the ficheiro parameter.	Patched by core rule	Y
CVE-2025-2154	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Echo Call Center Services Trade and Industry Inc. Specto CM allows Stored XSS.This issue affects Specto CM: before 17032025.	Patched by core rule	Y
CVE-2025-68605	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Post Grid and Gutenberg Blocks post-grid	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows Stored XSS.This issue affects Post Grid and Gutenberg Blocks: from n/a through <= 2.3.18.		
CVE-2025-68599	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Embeds For YouTube Plugin Support YouTube Embed youtube-embed allows Stored XSS.This issue affects YouTube Embed: from n/a through <= 5.4.	Patched by core rule	Y
CVE-2025-68598	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LiveComposer Page Builder: Live Composer live-composer-page-builder allows Stored XSS.This issue affects Page Builder: Live Composer: from n/a through <= 2.0.5.	Patched by core rule	Y
CVE-2025-68597	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BlueGlass Interactive AG Jobs for WordPress job-postings allows Stored XSS.This issue affects Jobs for WordPress: from n/a through <= 2.7.17.	Patched by core rule	Y
CVE-2025-68574	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in voidcoders WPBakery Visual Composer WHMCS Elements void-visual-whmcs-element allows DOM-Based XSS.This issue affects WPBakery Visual Composer WHMCS Elements: from n/a through <= 1.0.4.3.	Patched by core rule	Y
CVE-2025-68566	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wphocus My auctions allegro my-auctions-allegro-free-edition allows Stored XSS.This issue affects My auctions allegro: from n/a through <= 3.6.32.	Patched by core rule	Y
CVE-2025-68533	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes WC Builder wc-builder allows Stored XSS.This issue affects WC	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Builder: from n/a through <= 1.2.0.		
CVE-2025-68532	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in modeltheme ModelTheme Addons for WPBakery and Elementor modeltheme-addons-for-wpbakery allows Stored XSS.This issue affects ModelTheme Addons for WPBakery and Elementor: from n/a through < 1.5.6.	Patched by core rule	Y
CVE-2025-68528	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Free Shipping Bar: Amount Left for Free Shipping for WooCommerce amount-left-free-shipping-woocommerce allows Stored XSS.This issue affects Free Shipping Bar: Amount Left for Free Shipping for WooCommerce: from n/a through <= 2.4.9.	Patched by core rule	Y
CVE-2025-68527	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kodezen LLC Academy LMS academy allows Stored XSS.This issue affects Academy LMS: from n/a through <= 3.4.0.	Patched by core rule	Y
CVE-2025-68525	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pixelgrade Category Icon category-icon allows Stored XSS.This issue affects Category Icon: from n/a through <= 1.0.2.	Patched by core rule	Y
CVE-2025-68513	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in boldthemes Bold Timeline Lite bold-timeline-lite allows Stored XSS.This issue affects Bold Timeline Lite: from n/a through <= 1.2.7.	Patched by core rule	Y
CVE-2025-68512	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in creativeinteractivemedia Real 3D FlipBook real3d-flipbook-lite allows Stored XSS.This issue affects Real 3D FlipBook: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through <= 4.11.4.		
CVE-2025-68497	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Astra Widgets astra-widgets allows Stored XSS.This issue affects Astra Widgets: from n/a through <= 1.2.16.	Patched by core rule	Y
CVE-2025-67633	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brownbagmarketing Greenhouse Job Board greenhouse-job-board allows DOM-Based XSS.This issue affects Greenhouse Job Board: from n/a through <= 2.7.3.	Patched by core rule	Y
CVE-2025-67632	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The Plugin Factory Google AdSense for Responsive Design – GARD google-adsense-for-responsive-design-gard allows DOM-Based XSS.This issue affects Google AdSense for Responsive Design – GARD: from n/a through <= 2.23.	Patched by core rule	Y
CVE-2025-67631	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ecommerce Platforms Gift Hunt gift-hunt allows Stored XSS.This issue affects Gift Hunt: from n/a through <= 2.0.2.	Patched by core rule	Y
CVE-2025-67630	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webheadcoder WH Tweaks wh-tweaks allows Stored XSS.This issue affects WH Tweaks: from n/a through <= 1.0.2.	Patched by core rule	Y
CVE-2025-67629	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Basticom Basticom Framework basticom-framework allows Stored XSS.This issue affects Basticom Framework: from n/a through <= 1.5.2.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-67628	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AMP-MODE Review Disclaimer review-disclaimer allows Stored XSS.This issue affects Review Disclaimer: from n/a through <= 2.0.3.	Patched by core rule	Y
CVE-2025-67627	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TouchOfTech Draft Notify draft-notify allows Stored XSS.This issue affects Draft Notify: from n/a through <= 1.5.	Patched by core rule	Y
CVE-2023-32120	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting').	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Bob Hostel allows DOM-Based XSS.This issue affects Hostel: from n/a through 1.1.5.1.	Patched by core rule	Y
CVE-2025-66444	Cross-site Scripting vulnerability in Hitachi Infrastructure Analytics Advisor.	Cross-site Scripting vulnerability in Hitachi Infrastructure Analytics Advisor (Data Center Analytics component) and Hitachi Ops Center Analyzer (Hitachi Ops Center Analyzer detail view component).This issue affects Hitachi Infrastructure Analytics Advisor:; Hitachi Ops Center Analyzer: from 10.0.0-00 before 11.0.5-00.	Patched by core rule	Y
CVE-2025-15052	A vulnerability was detected in code-projects Student Information System 1.0.	A vulnerability was detected in code-projects Student Information System 1.0. This vulnerability affects unknown code of the file /profile.php. Performing manipulation of the argument firstname/lastname results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2021-47738	CSZ CMS 1.2.7 contains a persistent cross-site scripting vulnerability	CSZ CMS 1.2.7 contains a persistent cross-site scripting vulnerability that allows unauthorized users to embed malicious JavaScript in private messages. Attackers can send messages with script payloads in the user-agent header, which will execute when an admin views the message in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		backend dashboard.		
CVE-2021-47737	CSZ CMS 1.2.7 contains an HTML injection vulnerability	CSZ CMS 1.2.7 contains an HTML injection vulnerability that allows authenticated users to insert malicious hyperlinks in message titles. Attackers can craft POST requests to the member messaging system with HTML-based links to potentially conduct phishing or social engineering attacks.	Patched by core rule	Y
CVE-2021-47733	CMSimple 5.4 contains a cross-site scripting vulnerability	CMSimple 5.4 contains a cross-site scripting vulnerability that allows attackers to bypass input filtering by using HTML to Unicode encoding. Attackers can inject malicious scripts by encoding payloads like ')-alert(1)// and execute arbitrary JavaScript when victims interact with delete buttons.	Patched by core rule	Y
CVE-2021-47732	CMSimple 5.2 contains a stored cross-site scripting vulnerability	CMSimple 5.2 contains a stored cross-site scripting vulnerability in the Filebrowser External input field that allows attackers to inject malicious JavaScript. Attackers can place unfiltered JavaScript code that executes when users click on Page or Files tabs, enabling persistent script injection.	Patched by core rule	Y
CVE-2021-47716	Orangescrum 1.8.0 contains multiple cross-site scripting vulnerabilities	Orangescrum 1.8.0 contains multiple cross-site scripting vulnerabilities that allow authenticated attackers to inject malicious scripts through various input parameters. Attackers can exploit parameters like 'projid', 'CS_message', and 'name' to execute arbitrary JavaScript code in victim's browsers by submitting crafted payloads through application endpoints.	Patched by core rule	Y
CVE-2025-66845	A reflected Cross-Site Scripting (XSS) vulnerability has been identified in TechStore version 1.0.	A reflected Cross-Site Scripting (XSS) vulnerability has been identified in TechStore version 1.0. The user_name endpoint reflects the id query parameter directly into the HTML response without output encoding or sanitization, allowing execution of arbitrary JavaScript code in a victim闡ユ獨 browser.	Patched by core rule	Y
CVE-2025-13183	Improper Neutralization	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	of Input During Web Page Generation (XSS or 'Cross-site Scripting')	Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hotech Software Inc. Otello allows Stored XSS.This issue affects Otello: from 2.4.0 before 2.4.4.	rule	
CVE-2025-68559	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem Theme Elements (for Elementor).This issue affects TheGem Theme Elements (for Elementor): from n/a through 5.10.5.1.	Patched by core rule	Y
CVE-2025-68548	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebCodingPlace Responsive Posts Carousel Pro allows Stored XSS.This issue affects Responsive Posts Carousel Pro: from n/a through 15.2.	Patched by core rule	Y
CVE-2025-14635	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting.	The Happy Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ha_page_custom_js' parameter in all versions up to, and including, 3.20.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, despite the intended role restriction of Custom JS to Administrat	Patched by core rule	Y
CVE-2025-14000	The Membership Plugin Restrict Content plugin for WordPress is vulnerable to Stored XSS.	The Membership Plugin Restrict Content plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'register_form' and 'restrict' shortcodes in all versions up to, and including, 3.2.15 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14548	The Calendar plugin for	The Calendar plugin for	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	WordPress is vulnerable to Stored Cross-Site Scripting via the 'event_desc' parameter in all versions up to, and including, 1.3.16 due to insufficient input sanitization and output escaping.	WordPress is vulnerable to Stored Cross-Site Scripting via the 'event_desc' parameter in all versions up to, and including, 1.3.16 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page, granted they can convince an administrator to enable lower privilege users to manage calen	rule	
CVE-2025-68614	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Prior to version 25.12	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Prior to version 25.12.0, the Alert Rule API is vulnerable to stored cross-site scripting. Alert rules can be created or updated via LibreNMS API. The alert rule name is not properly sanitized, and can be used to inject HTML code. This issue has been patched in version 25.12.0.	Patched by core rule	Y
CVE-2025-67291	A stored cross-site scripting (XSS) vulnerability in the Media module of Piranha CMS v12.1	A stored cross-site scripting (XSS) vulnerability in the Media module of Piranha CMS v12.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name field.	Patched by core rule	Y
CVE-2025-67290	A stored cross-site scripting (XSS) vulnerability in the Page Settings module of Piranha CMS v12.1	A stored cross-site scripting (XSS) vulnerability in the Page Settings module of Piranha CMS v12.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Excerpt field.	Patched by core rule	Y
CVE-2025-65837	PublicCMS V5.202506.b is vulnerable to Cross Site Scripting (XSS)	PublicCMS V5.202506.b is vulnerable to Cross Site Scripting (XSS) in the Content Search module.	Patched by core rule	Y
CVE-2025-65790	A reflected cross-site scripting (XSS) vulnerability exists in FuguHub 8.1 when serving SVG files	A reflected cross-site scripting (XSS) vulnerability exists in FuguHub 8.1 when serving SVG files through the /fs/ file manager interface. FuguHub does not sanitize or restrict script execution inside SVG content. When a victim opens a crafted SVG containing an inline <script> element, the browser	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		executes the attacker-controlled JavaScript.		
CVE-2024-25812	MyNET up to v26.05 was discovered to contain a reflected cross-site scripting (XSS) vulnerability	MyNET up to v26.05 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the src parameter.	Patched by core rule	Y
CVE-2024-35321	MyNET up to v26.08 was discovered to contain a Reflected cross-site scripting (XSS) vulnerability	MyNET up to v26.08 was discovered to contain a Reflected cross-site scripting (XSS) vulnerability via the msgtipo parameter.	Patched by core rule	Y
CVE-2024-25814	MyNET up to v26.05 was discovered to contain a reflected cross-site scripting (XSS) vulnerability vi	MyNET up to v26.05 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the msg parameter.	Patched by core rule	Y
CVE-2025-67289	An arbitrary file upload vulnerability in the Attachments module of Frappe Framework v15.89.0	An arbitrary file upload vulnerability in the Attachments module of Frappe Framework v15.89.0 allows attackers to execute arbitrary code via uploading a crafted XML file.	Patched by core rule	Y
CVE-2025-65270	Reflected cross-site scripting (XSS) vulnerability in ClinCapture EDC 3.0 and 2.2.3	Reflected cross-site scripting (XSS) vulnerability in ClinCapture EDC 3.0 and 2.2.3, allowing an unauthenticated remote attacker to execute JavaScript code in the context of the victim's browser.	Patched by core rule	Y
CVE-2025-67443	Schlix CMS before v2.2.9-5 is vulnerable to Cross Site Scripting (XSS).	Schlix CMS before v2.2.9-5 is vulnerable to Cross Site Scripting (XSS). Due to lack of javascript sanitization in the login form, incorrect login attempts in logs are triggered as XSS in the admin panel.	Patched by core rule	Y
CVE-2025-8460	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Notification rules, Open tickets module) allows Stored XSS by users with elevated privileges.This issue affects Infra Monitoring: from 24.10.0 before 24.10.5, from 24.04.0 before 24.04.5, from 23.10.0 before 23.10.4.	Patched by core rule	Y
CVE-2025-54890	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Centreon Infra Monitoring (Hostgroup configuration	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		page) allows Stored XSS by users with elevated privileges.This issue affects Infra Monitoring: from 24.10.0 before 24.10.15, from 24.04.0 before 24.04.19, from 23.10.0 before 23.10.29.		
CVE-2025-62094	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Voidthemes Void Elementor WHMCS Elements For Elementor Page Builder.This issue affects Void Elementor WHMCS Elements For Elementor Page Builder: from n/a through 2.0.1.2.	Patched by core rule	Y
CVE-2025-14855	The SureForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting	The SureForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form field parameters in all versions up to, and including, 2.2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-9343	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress	The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via ticket subjects in all versions up to, and including, 3.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14151	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'outbound_resource' parameter in the slimtrack AJAX action in all versions up to, and including, 5.3.2. This is due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		accesses an injected page.		
CVE-2025-11747	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting	The Colibri Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the colibri_blog_posts shortcode in all versions up to, and including, 1.0.345 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-66522	A stored cross-site scripting (XSS) vulnerability exists in the Digital IDs functionality	A stored cross-site scripting (XSS) vulnerability exists in the Digital IDs functionality of the Foxit PDF Editor Cloud (pdfonline.foxit.com). The application does not properly sanitize or encode the Common Name field of Digital IDs before inserting user-supplied content into the DOM. As a result, embedded HTML or JavaScript may execute whenever the Digital IDs dialog is accessed or when the affected PDF is loaded.	Patched by core rule	Y
CVE-2025-66521	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Trusted Certificates feature. A crafted payload can be injected as the certificate name, which is later rendered into the DOM without proper sanitization. As a result, the injected script executes each time the Trusted Certificates view is loaded.	Patched by core rule	Y
CVE-2025-66520	A stored cross-site scripting (XSS) vulnerability exists in the Portfolio feature	A stored cross-site scripting (XSS) vulnerability exists in the Portfolio feature of the Foxit PDF Editor cloud (pdfonline.foxit.com). User-supplied SVG files are not properly sanitized or validated before being inserted into the HTML structure. As a result, embedded HTML or JavaScript within a crafted SVG may execute whenever the Portfolio file list is rendered.	Patched by core rule	Y
CVE-2025-66519	A stored cross-site scripting (XSS)	A stored cross-site scripting (XSS) vulnerability exists in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability exists in pdfonline.foxit.com	pdfonline.foxit.com within the Layer Import functionality. A crafted payload can be injected into the reate new Layer field during layer import and is later rendered into the DOM without proper sanitization. As a result, the injected script executes when the Layers panel is accessed.		
CVE-2025-66502	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Page Templates feature.	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Page Templates feature. A crafted payload can be stored as the template name, which is later rendered into the DOM without proper sanitization. As a result, the injected script executes each time the affected PDF is loaded.	Patched by core rule	Y
CVE-2025-66501	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Predefine Text feature of the Foxit eSign section.	A stored cross-site scripting (XSS) vulnerability exists in pdfonline.foxit.com within the Predefined Text feature of the Foxit eSign section. A crafted payload can be stored via the Identity field, which is later rendered into the DOM without proper sanitization. As a result, the injected script may execute when predefined text is used or when viewing document properties.	Patched by core rule	Y
CVE-2025-66500	A stored cross-site scripting (XSS) vulnerability exists in webplugins.foxit.com.	A stored cross-site scripting (XSS) vulnerability exists in webplugins.foxit.com. A postMessage handler fails to validate the message origin and directly assigns externalPath to a script source, allowing an attacker to execute arbitrary JavaScript when a crafted postMessage is received.	Patched by core rule	Y
CVE-2025-14449	The BA Book Everything plugin for WordPress is vulnerable to Stored Cross-Site Scripting	The BA Book Everything plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's babe-search-form shortcode in all versions up to, and including, 1.8.14 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-64675	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Cosmos	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Cosmos DB allows an unauthorized attacker to perform spoofing over a network.	Patched by core rule	Y
CVE-2025-64677	Improper neutralization of input during web page generation ('cross-site scripting') in Office Out-o	Improper neutralization of input during web page generation ('cross-site scripting') in Office Out-of-Box Experience allows an unauthorized attacker to perform spoofing over a network.	Patched by core rule	Y
CVE-2025-68147	Open Source Point of Sale (opensourcepos) is a web based point of sale application written in PHP us	Open Source Point of Sale (opensourcepos) is a web based point of sale application written in PHP using CodeIgniter framework. Starting in version 3.4.0 and prior to version 3.4.2, a Stored Cross-Site Scripting (XSS) vulnerability exists in the "Return Policy" configuration field. The application does not properly sanitize user input before saving it to the database or displaying it on receipts. An attacker with access to the "Store Configuration" (such as a rogue administrator or an account com	Patched by core rule	Y
CVE-2025-65778	An issue was discovered in Wekan The Open Source kanban board system up to version 18.15	An issue was discovered in Wekan The Open Source kanban board system up to version 18.15, fixed in 18.16. Uploaded attachments can be served with attacker-controlled Content-Type (text/html), allowing execution of attacker-supplied HTML/JS in the application's origin and enabling session/token theft and CSRF actions.	Patched by core rule	Y
CVE-2025-12570	The Fancy Product Designer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG	The Fancy Product Designer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 6.4.8 due to insufficient input sanitization and output escaping in the data-to-image.php and pdf-to-image.php files. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-41752	An XSS vulnerability in pxc_portSfp.php can be used by an unauthenticated remote attacker	An XSS vulnerability in pxc_portSfp.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is	Patched by core rule	Y
CVE-2025-41751	An XSS vulnerability in pxc_portCntr.php can be used by an unauthenticated remote attacker	An XSS vulnerability in pxc_portCntr.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is	Patched by core rule	Y
CVE-2025-41750	An XSS vulnerability in pxc_PortCfg.php can be used by an unauthenticated remote attacker	An XSS vulnerability in pxc_PortCfg.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is	Patched by core rule	Y
CVE-2025-41749	An XSS vulnerability in port_util.php can be used by an unauthenticated remote attacker	An XSS vulnerability in port_util.php can be used by an unauthenticated remote attacker to trick an authenticated user to click	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is se		
CVE-2025-41748	An XSS vulnerability in pxc_Dot1xCfg.php can be used by an unauthenticated remote attacker	An XSS vulnerability in pxc_Dot1xCfg.php can be used by an unauthenticated remote attacker to trick an authenticated user to click on the link provided by the attacker in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is	Patched by core rule	Y
CVE-2025-41747	An XSS vulnerability in pxc_vlanIntfCfg.php can be used by an unauthenticated remote attacker	An XSS vulnerability in pxc_vlanIntfCfg.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session coo	Patched by core rule	Y
CVE-2025-41746	An XSS vulnerability in pxc_portSecCfg.php can be used by an unauthenticated remote attacker	An XSS vulnerability in pxc_portSecCfg.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cook		
CVE-2025-41745	An XSS vulnerability in pxc_portCntr2.php can be used by an unauthenticated remote attacker	An XSS vulnerability in pxc_portCntr2.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cooki	Patched by core rule	Y
CVE-2025-41695	An XSS vulnerability in dyn_conn.php can be used by an unauthenticated remote attacker	An XSS vulnerability in dyn_conn.php can be used by an unauthenticated remote attacker to trick an authenticated user to send a manipulated POST request to the device in order to change parameters available via web based management (WBM). The vulnerability does not provide access to system-level resources such as operating system internals or privileged functions. Access is limited to device configuration parameters that are available in the context of the web application. The session cookie is	Patched by core rule	Y
CVE-2025-13604	The Login Security, FireWall, Malware removal by CleanTalk plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the page URL in all versions up to, and including, 2.168 due to insufficient input sanitization and output escaping.	The Login Security, FireWall, Malware removal by CleanTalk plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the page URL in all versions up to, and including, 2.168 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-12705	The Social Reviews & Recommendations plugin for WordPress is vulnerable to Stored Cross-Site Scripting.	The Social Reviews & Recommendations plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in the 'trim_text' function in all versions up to, and including, 2.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in version 2.5.	Patched by core rule	Y
CVE-2025-13639	Inappropriate implementation in WebRTC in Google Chrome prior to 143.0.7499.41 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page.	Inappropriate implementation in WebRTC in Google Chrome prior to 143.0.7499.41 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: Low)	Patched by core rule	Y

INDUSFACE™

Indusface is a leading application security SaaS company, securing over 5,000 customers across 95 countries with its award-winning platform. Funded by institutional investors, it has been a category leader in Gartner Peer Insights™ for the past three years.

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

Gartner Peer Insights Customers' Choice 2024

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

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

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