INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

February 2025

The total zero-day vulnerabilities count for February month: 473

Command Injection	SQL Injection	SSRF	Malicious File Upload	Cross-Site Scripting	XML External Entity
27	118	2	7	293	2

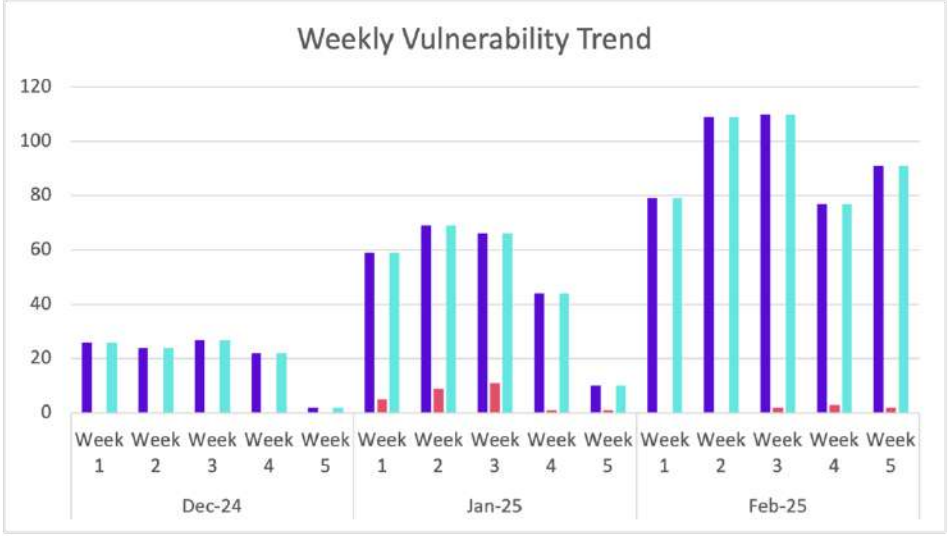
Zero-day vulnerabilities protected through core rules	466
Zero-day vulnerabilities protected through custom rules	7
Zero-day vulnerabilities found by Indusface WAS	466

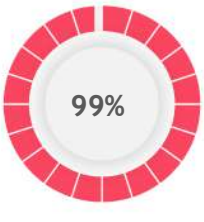
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

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

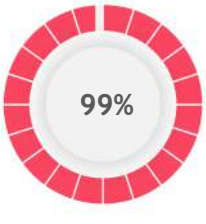
Weekly Vulnerability Trend





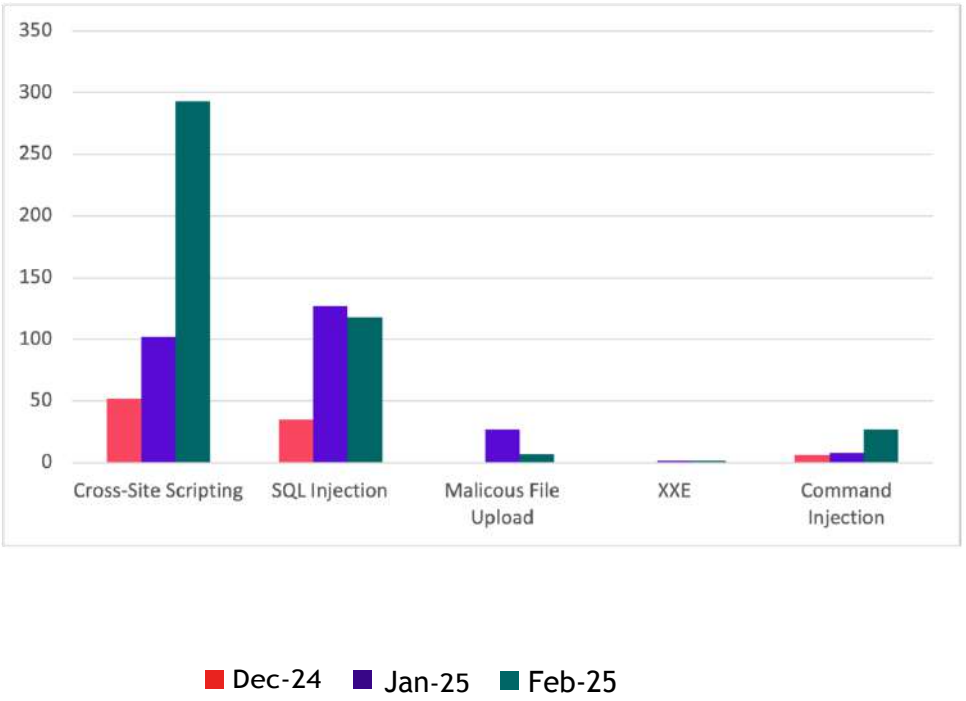
of the zero-day vulnerabilities were protected by the core rules in the last month

of the zero-day vulnerabilities were protected by the custom 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-2024-10001	Code Injection Vulnerability in GitHub Enterprise Server Allows Arbitrary Code Execution via Message Handling	A Code Injection vulnerability was identified in GitHub Enterprise Server that allowed attackers to inject malicious code into the query selector via the identity property in the message handling function. This enabled the exfiltration of sensitive data by manipulating the DOM, including authentication tokens. To execute the attack, the victim must be logged into GitHub and interact with the attacker controlled malicious webpage containing the hidden iframe. This vulnerability occurs due to an improper sequence of validation, where the origin check occurs after accepting the user-controlled identity property. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.11.16, 3.12.10, 3.13.5, 3.14.2, and 3.15.0. This vulnerability was reported via the GitHub Bug Bounty program.	Patched by core rule	Y
CVE-2024-13869	Migration, Backup, Staging – WPvivid <= 0.9.112 - Authenticated (Admin+) Arbitrary File Upload via wpvivid_upload_file	The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_files' function in all versions up to, and including, 0.9.112. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affected site's server which may make remote code execution possible. NOTE: Uploaded files are only accessible on WordPress instances running on the NGINX web server as the existing .htaccess within the target file upload folder prevents access on Apache servers.		
CVE-2025-0108	PAN-OS: Authentication Bypass in the Management Web Interface	An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts. While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS. You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practices deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue does not affect Cloud NGFW or Prisma Access software.	Patched by core rule	Y
CVE-2025-0798	MicroWorld eScan Antivirus Quarantine rtscanner os command injection	A vulnerability was found in MicroWorld eScan Antivirus 7.0.32 on Linux. It has been rated as critical. This issue affects some unknown processing of the file rtscanner of the component Quarantine Handler. The manipulation leads to os command injection. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0868	Remote Code Execution in DocsGPT	A vulnerability, that could result in Remote Code Execution (RCE), has been found in DocsGPT. Due to improper parsing of JSON data using eval() an unauthorized attacker could send arbitrary Python code to be executed via /api/remote endpoint. This issue affects DocsGPT: from 0.8.1 through 0.12.0.	Patched by core rule	Y
CVE-2025-1128	Everest Forms <= 3.0.9.4 - Unauthenticated Arbitrary	The Everest Forms – Contact Forms, Quiz, Survey,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	File Upload, Read, and Deletion	Newsletter & Payment Form Builder for WordPress plugin for WordPress is vulnerable to arbitrary file upload, read, and deletion due to missing file type and path validation in the 'format' method of the EVF_Form_Fields_Upload class in all versions up to, and including, 3.0.9.4. This makes it possible for unauthenticated attackers to upload, read, and delete arbitrary files on the affected site's server which may make remote code execution, sensitive information disclosure, or a site takeover possible.		
CVE-2025-1229	olajowon Loggrove page os command injection	A vulnerability classified as critical was found in olajowon Loggrove up to e428fac38cc480f011afcb1d8ce6c2bad378ddd6. Affected by this vulnerability is an unknown functionality of the file /read/?page=1&logfile=eee&match=. The manipulation of the argument path leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Patched by core rule	Y
CVE-2025-1339	TOTOLINK X18 cstecgi.cgi setL2tpdConfig os command injection	A vulnerability was found in TOTOLINK X18 9.1.0cu.2024_B20220329. It has been rated as critical. This issue affects the function setL2tpdConfig of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument enable leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1369	MicroWord eScan Antivirus USB Password os command injection	A vulnerability classified as critical was found in MicroWord eScan Antivirus 7.0.32 on Linux. Affected by this vulnerability is an unknown functionality of the component USB Password Handler. The manipulation leads to os command injection. The attack needs to be approached locally. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1370	MicroWorld eScan Antivirus Autoscan USB epsdaemon sprintf os command injection	A vulnerability, which was classified as critical, has been found in MicroWorld eScan Antivirus 7.0.32 on	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Linux. Affected by this issue is the function sprintf of the file epsdaemon of the component Autoscan USB. The manipulation leads to os command injection. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1448	Synway SMG Gateway Management Software 9-12ping.php command injection	A vulnerability was found in Synway SMG Gateway Management Software up to 20250204. It has been rated as critical. This issue affects some unknown processing of the file 9-12ping.php. The manipulation of the argument retry leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1465	lmxcms Maintenance db.inc.php code injection	A vulnerability, which was classified as problematic, was found in lmxcms 1.41. Affected is an unknown function of the file db.inc.php of the component Maintenance. The manipulation leads to code injection. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1536	Raisecom Multi-Service Intelligent Gateway Request Parameter vpn_template_style.php os command injection	A vulnerability was found in Raisecom Multi-Service Intelligent Gateway up to 20250208. It has been declared as critical. This vulnerability affects unknown code of the file /vpn/vpn_template_style.php of the component Request Parameter Handler. The manipulation of the argument stylenum leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1546	BDCOM Behavior Management and Auditing System operate.mds log_operate_clear os command injection	A vulnerability has been found in BDCOM Behavior Management and Auditing System up to 20250210 and classified as critical. Affected by this vulnerability is the function log_operate_clear of the file /webui/modules/log/operate.mds. The manipulation of the argument start_code leads to os command injection. The attack can be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1676	hzmanyun Education and Training System pdf2swf os command injection	A vulnerability classified as critical was found in hzmanyun Education and Training System 3.1.1. Affected by this vulnerability is the function pdf2swf of the file /pdf2swf. The manipulation of the argument file leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-20029	BIG-IP iControl REST and tmsh vulnerability	Command injection vulnerability exists in iControl REST and BIG-IP TMOS Shell (tmsh) save command, which may allow an authenticated attacker to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	Patched by core rule	Y
CVE-2025-22604	Cacti has Authenticated RCE via multi-line SNMP responses	Cacti is an open source performance and fault management framework. Due to a flaw in multi-line SNMP result parser, authenticated users can inject malformed OIDs in the response. When processed by ss_net_snmp_disk_io() or ss_net_snmp_disk_bytes(), a part of each OID will be used as a key in an array that is used as part of a system command, causing a command execution vulnerability. This vulnerability is fixed in 1.2.29.	Patched by core rule	Y
CVE-2025-23217	Mitmweb API Authentication Bypass Using Proxy Server	mitmproxy is a interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers and mitmweb is a web-based interface for mitmproxy. In mitmweb 11.1.1 and below, a malicious client can use mitmweb's proxy server (bound to `*:8080` by default) to access mitmweb's internal API (bound to `127.0.0.1:8081` by default). In other words, while the cannot access the API directly, they can access the API through the proxy. An attacker may be able to escalate this SSRF-style access to remote code execution. The mitmproxy and mitmdump tools are unaffected. Only mitmweb is affected. This vulnerability has been fixed in mitmproxy 11.1.2 and above. Users are	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-24016	Remote code execution in Wazuh server	Wazuh is a free and open source platform used for threat prevention, detection, and response. Starting in version 4.4.0 and prior to version 4.9.1, an unsafe deserialization vulnerability allows for remote code execution on Wazuh servers. DistributedAPI parameters are a serialized as JSON and deserialized using `as_wazuh_object` (in `framework/wazuh/core/cluster/common.py`). If an attacker manages to inject an unsanitized dictionary in DAPI request/response, they can forge an unhandled exception (`__unhandled_exc__`) to evaluate arbitrary python code. The vulnerability can be triggered by anybody with API access (compromised dashboard or Wazuh servers in the cluster) or, in certain configurations, even by a compromised agent. Version 4.9.1 contains a fix.	Patched by core rule	Y
CVE-2025-24959	Environment Variable Injection for dotenv API in zx	zx is a tool for writing better scripts. An attacker with control over environment variable values can inject unintended environment variables into `process.env`. This can lead to arbitrary command execution or unexpected behavior in applications that rely on environment variables for security-sensitive operations. Applications that process untrusted input and pass it through `dotenv.stringify` are particularly vulnerable. This issue has been patched in version 8.3.2. Users should immediately upgrade to this version to mitigate the vulnerability. If upgrading is not feasible, users can mitigate the vulnerability by sanitizing user-controlled environment variable values before passing them to `dotenv.stringify`. Specifically, avoid using `"`, `'`, and backticks in values, or enforce strict validation of environment variables before usage.	Patched by core rule	Y
CVE-2025-24971	OS Command Injection endpoint '/upload/init' parameter 'filename' (RCE) in DumpDrop	DumpDrop is a stupid simple file upload application that provides an interface for dragging and dropping files. An OS Command Injection vulnerability was discovered in the DumbDrop application, `/upload/init` endpoint. This vulnerability could allow an attacker to execute arbitrary code remotely when the **Apprise Notification** enabled. This issue has been addressed in commit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		`4ff8469d` and all users are advised to patch. There are no known workarounds for this vulnerability.		
CVE-2025-26613	OS Command Injection endpoint 'gerenciar_backup.php' parameter 'file' (RCE) in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. An OS Command Injection vulnerability was discovered in the WeGIA application, `gerenciar_backup.php` endpoint. This vulnerability could allow an attacker to execute arbitrary code remotely. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-27106	Code injection in binance-trading-bot	binance-trading-bot is an automated Binance trading bot with trailing buy/sell strategy. Authenticated users of binance-trading-bot can achieve Remote Code Execution on the host system due to a command injection vulnerability in the `/restore` endpoint. The restore endpoint of binance-trading-bot is vulnerable to command injection via the `/restore` endpoint. The name of the uploaded file is passed to shell.exec without sanitization other than path normalization, resulting in Remote Code Execution. This may allow any authorized user to execute code in the context of the host machine. This issue has been addressed in version 0.0.100 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-27140	WeGIA vulnerable to OS Command Injection at endpoint 'importar_dump.php' parameter 'import' (RCE)	WeGIA is a Web manager for charitable institutions. An OS Command Injection vulnerability was discovered in versions prior to 3.2.15 of the WeGIA application, `importar_dump.php` endpoint. This vulnerability could allow an attacker to execute arbitrary code remotely. The command is basically a command to move a temporary file, so a webshell upload is also possible. Version 3.2.15 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-27142	LocalSend path traversal vulnerability in the file upload endpoint allows nearby devices to execute arbitrary commands	LocalSend is a free, open-source app that allows users to securely share files and messages with nearby devices over their local network without needing an internet connection. Prior to version 1.17.0, due to the missing sanitization of the path in the `POST /api/localsend/v2/prepare-upload` and the `POST /api/localsend/v2/upload` endpoint, a malicious file transfer request can write files to the arbitrary location	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		on the system, resulting in the remote command execution. A malicious file transfer request sent by nearby devices can write files into an arbitrary directory. This usually allows command execution via the startup folder on Windows or Bash-related files on Linux. If the user enables the `Quick Save` feature, it will silently write files without explicit user interaction. Version 1.17.0 fixes this issue.		
CVE-2025-27146	Matrix IRC Bridge allows IRC command injection to own puppeted user	matrix-appservice-irc is a Node.js IRC bridge for Matrix. The matrix-appservice-irc bridge up to version 3.0.3 contains a vulnerability which can lead to arbitrary IRC command execution as the puppeted user. The attacker can only inject commands executed as their own IRC user. The vulnerability has been patched in matrix-appservice-irc version 3.0.4.	Patched by core rule	Y
CVE-2025-27364	N/A	In MITRE Caldera through 4.2.0 and 5.0.0 before 35bc06e, a Remote Code Execution (RCE) vulnerability was found in the dynamic agent (implant) compilation functionality of the server. This allows remote attackers to execute arbitrary code on the server that Caldera is running on via a crafted web request to the Caldera server API used for compiling and downloading of Caldera's Sandcat or Manx agent (implants). This web request can use the gcc -extldflags linker flag with sub-commands.	Patched by core rule	Y

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-1165	Lumsoft ERP FileUploadApi.ashx DoWebUpload unrestricted upload	A vulnerability, which was classified as critical, was found in Lumsoft ERP 8. Affected is the function DoUpload/DoWebUpload of the file /Api/FileUploadApi.ashx. The manipulation of the argument file 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 custom rule	N
CVE-2025-1166	SourceCodester Food Menu Manager update.php unrestricted upload	A vulnerability has been found in SourceCodester Food Menu Manager 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file endpoint/update.php. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by custom rule	N
CVE-2025-1555	hzmanyun Education and Training System saveImage unrestricted upload	A vulnerability classified as critical was found in hzmanyun Education and Training System 3.1.1. This vulnerability affects the function saveImage. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by custom rule	N
CVE-2025-1598	SourceCodester Best Church Management Software asset_crud.php unrestricted upload	A vulnerability was found in SourceCodester Best Church Management Software 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/app/asset_crud.php. The manipulation of the argument photo1 leads to unrestricted upload. The attack can be launched remotely. The exploit has	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1646	Lumsoft ERP ASPX File UploadAjaxAPI.ashx unrestricted upload	A vulnerability, which was classified as critical, has been found in Lumsoft ERP 8. Affected by this issue is some unknown functionality of the file /Api/TinyMce/UploadAjaxAPI.ashx of the component ASPX File Handler. The manipulation of the argument file leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by custom rule	N
CVE-2025-22654	WordPress Simplified Plugin Plugin <= 1.0.6 - Arbitrary File Upload vulnerability	Unrestricted Upload of File with Dangerous Type vulnerability in kodeshpa Simplified allows Using Malicious Files. This issue affects Simplified: from n/a through 1.0.6.	Patched by custom rule	N
CVE-2024-13869	Migration, Backup, Staging – WPvivid <= 0.9.112 - Authenticated (Admin+) Arbitrary File Upload via wpvivid_upload_file	The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload_files' function in all versions up to, and including, 0.9.112. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. NOTE: Uploaded files are only accessible on WordPress instances running on the NGINX web server as the existing .htaccess within the target file upload folder prevents access on Apache servers.	Patched by custom rule	N

Server-side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-13879	Stream <= 4.0.2 - Authenticated (Admin+) Server-Side Request Forgery	The Stream plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.0.2 due to insufficient validation on the webhook feature. This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application which can be used to query and modify information from internal services.	Patched by core rule	Y
CVE-2025-1447	kasuganosoras Pigeon index.php server-side request forgery	A vulnerability was found in kasuganosoras Pigeon 1.0.177. It has been declared as critical. This vulnerability affects unknown code of the file /pigeon/imgproxy/index.php. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. Upgrading to version 1.0.181 is able to address this issue. The patch is identified as 84cea5fe73141689da2e7ec8676d47435bd6423e. It is recommended to upgrade the affected component.	Patched by core rule	Y

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-6195	Server-Side Request Forgery (SSRF) in GitLab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.5 prior to 16.9.7, starting from 16.10 prior to 16.10.5, and starting from 16.11 prior to 16.11.2. GitLab was vulnerable to Server Side Request Forgery when an attacker uses a malicious URL in the markdown image value when importing a GitHub repository.	Patched by core rule	Y
CVE-2024-13791	Bit Assist <= 1.5.2 - Path Traversal to Authenticated (Administrator+) Arbitrary File Read via downloadResponse File Function	Bit Assist plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.5.2 via the downloadResponseFile() function. This makes it possible for authenticated attackers, with Administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	Patched by core rule	Y
CVE-2025-0851	Path traversal issue in Deep Java Library	A path traversal issue in ZipUtils.unzip and TarUtils.untar in Deep Java Library (DJL) on all platforms allows a bad actor to write files to arbitrary locations.	Patched by core rule	Y
CVE-2025-0859	Post and Page Builder by BoldGrid <= 1.27.6 - Path Traversal to Authenticated (Contributor+) Arbitrary File Read via template_via_url Function	The Post and Page Builder by BoldGrid – Visual Drag and Drop Editor plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.27.6 via the template_via_url() function. This makes it	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible for authenticated attackers, with Contributor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.		
CVE-2025-0973	CmsEasy index.php backAll_action path traversal	A vulnerability classified as critical was found in CmsEasy 7.7.7.9. This vulnerability affects the function backAll_action in the library lib/admin/database_admin.php of the file /index.php?case=database&act=backAll&admin_dir=admin&site=default. The manipulation of the argument select[] leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1106	CmsEasy database_admin.php restore_action path traversal	A vulnerability classified as critical has been found in CmsEasy 7.7.7.9. This affects the function deletedir_action/restore_action in the library lib/admin/database_admin.php. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		way.		
CVE-2025-1226	ywoa setup.jsp improper authorization	A vulnerability was found in ywoa up to 2024.07.03. It has been declared as critical. This vulnerability affects unknown code of the file /oa/setup/setup.jsp. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-1228	olajowon Loggrove Logfile Update page path traversal	A vulnerability classified as problematic has been found in olajowon Loggrove up to e428fac38cc480f011afcb1d8ce6c2bad378ddd6. Affected is an unknown function of the file /read/?page=1&logfile=LOG_Monitor of the component Logfile Update Handler. The manipulation of the argument path leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	Patched by core rule	Y
CVE-2025-1335	CmsEasy file_admin.php	A vulnerability, which was classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	deleteimg_action path traversal	problematic, was found in CmsEasy 7.7.7.9. Affected is the function deleteimg_action in the library lib/admin/file_admin.php. The manipulation of the argument imgname leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1336	CmsEasy image_admin.php deleteimg_action path traversal	A vulnerability has been found in CmsEasy 7.7.7.9 and classified as problematic. Affected by this vulnerability is the function deleteimg_action in the library lib/admin/image_admin.php. The manipulation of the argument imgname leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1543	iteachyou Dreamer CMS ueditor-1.4.3.3 path traversal	A vulnerability, which was classified as problematic, has been found in iteachyou Dreamer CMS 4.1.3. This issue affects some unknown processing of the file /resource/js/ueditor-1.4.3.3. The manipulation leads to path traversal. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1584	opensolon Solon StaticMappings.java path traversal	A vulnerability classified as problematic was found in opensolon Solon up to 3.0.8. This vulnerability affects unknown code of the file solon-projects/solon-web/solon-web-staticfiles/src/main/java/org/noear/solon/web/staticfiles/StaticMappings.java. The manipulation leads to path traversal: '../filedir'. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.0.9 is able to address this issue. The name of the patch is f46e47fd1f8455b9467d7ead3cdb0509115b2ef1. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-1588	PHPGurukul Online Nurse Hiring System manage-nurse.php path traversal	A vulnerability has been found in PHPGurukul Online Nurse Hiring System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/manage-nurse.php. The manipulation of the argument profilepic leads to path traversal: '../filedir'. The attack can be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting vulnerability classes.		
CVE-2025-1599	SourceCodester Best Church Management Software profile_crud.php path traversal	A vulnerability was found in SourceCodester Best Church Management Software 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/app/profile_crud.php. The manipulation of the argument old_cat_img leads to path traversal: '../filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-24786	Path traversal opening Sqlite3 database in WhoDB	WhoDB is an open source database management tool. While the application only displays Sqlite3 databases present in the directory `/db`, there is no path traversal prevention in place. This allows an unauthenticated attacker to open any Sqlite3 database present on the host machine that the application is running on. Affected versions of WhoDB allow users to connect to Sqlite3 databases. By default, the databases must be present in `/db/`	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		(or alternatively `./tmp/` if development mode is enabled). If no databases are present in the default directory, the UI indicates that the user is unable to open any databases. The database file is an user-controlled value. This value is used in `.Join()` with the default directory, in order to get the full path of the database file to open. No checks are performed whether the database file that is eventually opened actually resides in the default directory `/db`. This allows an attacker to use path traversal (`../../`) in order to open any Sqlite3 database present on the system. This issue has been addressed in version 0.45.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-24807	Fast DDS does not verify Permissions CA	eprosima Fast DDS is a C++ implementation of the DDS (Data Distribution Service) standard of the OMG (Object Management Group). Prior to versions 2.6.10, 2.10.7, 2.14.5, 3.0.2, 3.1.2, and 3.2.0, per design, PermissionsCA is not full chain validated, nor is the expiration date validated. Access control plugin validates only the S/MIME signature which causes an expired PermissionsCA to be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		taken as valid. Even though this issue is responsible for allowing `governance/permissions` from an expired PermissionsCA and having the system crash when PermissionsCA is not self-signed and contains the full-chain, the impact is low. Versions 2.6.10, 2.10.7, 2.14.5, 3.0.2, 3.1.2, and 3.2.0 contain a fix for the issue.		
CVE-2025-24888	Path traversal in SecureDrop Client API.download_reply()	The SecureDrop Client is a desktop application for journalists to communicate with sources and work with submissions on the SecureDrop Workstation. Prior to version 0.14.1, a malicious SecureDrop Server could obtain code execution on the SecureDrop Client virtual machine (`sd-app`). SecureDrop Server itself has multiple layers of built-in hardening, and is a dedicated physical machine exposed on the internet only via Tor hidden services for the Source and Journalist interfaces, and optionally via remote SSH access over another Tor hidden service. A newsroom's SecureDrop Workstation communicates only with its own dedicated SecureDrop Server. The SecureDrop Client runs in a dedicated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Qubes virtual machine, named `sd-app`, as part of the SecureDrop Workstation. The private OpenPGP key used to decrypt submissions and replies is stored in a separate virtual machine and never accessed directly. The vulnerability lies in the code responsible for downloading replies. The filename of the reply is obtained from the `Content-Disposition` HTTP header and used to write the encrypted reply on disk. Note that filenames are generated and sanitized server-side, and files are downloaded in an encrypted format, so a remote attacker who has not achieved server compromise, such as one posing as a source, could not craft the HTTP response necessary for this attack. While the filename is later checked to guard against path traversal before being moved into the Client's data storage directory, the file has already been written to a potentially arbitrary location. In this case, `safe_move()` would detect the path traversal and fail, leaving the original downloaded file in the attacker-chosen directory. Code execution can be gained by writing an autostart file in `/home/user/.config/a		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		utostart/`. Version 0.14.1 fixes the issue. As of time of publication, there is no known evidence of exploitation in the wild. This attack requires a previously compromised SecureDrop Server.		
CVE-2025-24889	Path traversal in sd-log Qubes virtual machine	The SecureDrop Client is a desktop application for journalists to communicate with sources and work with submissions on the SecureDrop Workstation. Prior to versions 0.14.1 and 1.0.1, an attacker who has already gained code execution in a virtual machine on the SecureDrop Workstation could gain code execution in the `sd-log` virtual machine by sending a specially crafted log entry. The vulnerability is not exploitable remotely and requires an attacker to already have code execution on one of the other virtual machines (VMs) of the system. Due to the Workstation's underlying usage of Qubes for strong isolation, the vulnerability would have allowed lateral movement between any log-enabled VM and the `sd-log` VM, but no further. The SecureDrop workstation collects logs centrally in an isolated virtual machine named `sd-log` for easy export for support and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		debugging purposes. The `sd-log` VM is completely isolated from the internet and ingests logs via a narrow Qubes RPC policy that allows for specific inter-VM communication via the Xen vchan protocol used by Qubes's qrexec mechanism. A path traversal bug was found in the logic used to choose where to write the log file for a specific VM: the VM name, used unsanitized in the destination path in `sd-log`, is supplied by the logging VM itself instead of being read from a trusted source, such as the Qubes environment variable `QREXEC_REMOTE_DOMAIN` that is used in the fixed implementation. An attacker could provide an arbitrary source VM name, possibly overwriting logs of other VMs, or writing a file named `syslog.log`, with attacker-controlled content, in arbitrary directories as a low-privileged user. A successful attack could potentially overwrite or add configuration to software that loads configuration files from a directory. This is exploitable to achieve code execution by setting the target directory to `/home/user/.config/autostart/` and letting it write `syslog.log`, because XFCE treats any file in that		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		directory as a `.desktop` file regardless of its extension. Versions 0.14.1 and 1.0.1 contain a patch for this issue.		
CVE-2025-24899	Disclosure of Sensitive User Information via API in reNgine	reNgine is an automated reconnaissance framework for web applications. A vulnerability was discovered in reNgine, where **an insider attacker with any role** (such as Auditor, Penetration Tester, or Sys Admin) **can extract sensitive information from other reNgine users.** After running a scan and obtaining vulnerabilities from a target, the attacker can retrieve details such as `username`, `password`, `email`, `role`, `first name`, `last name`, `status`, and `activity information` by making a GET request to `/api/listVulnerability/`. This issue has been addressed in version 2.2.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-24960	Missing Input validation for filename in backups endpoint in Jellystat	Jellystat is a free and open source Statistics App for Jellyfin. In affected versions Jellystat is directly using a user input in the route(s). This can lead to Path Traversal Vulnerabilities. Since this functionality is only for admin(s), there is very little scope for abuse. However, the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		`DELETE` `files/:filename` can be used to delete any file. This issue has been addressed in version 1.1.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-25163	WordPress Plugin A/B Image Optimizer Plugin <= 3.3 - Arbitrary File Download vulnerability	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Zach Swetz Plugin A/B Image Optimizer allows Path Traversal. This issue affects Plugin A/B Image Optimizer: from n/a through 3.3.	Patched by core rule	Y
CVE-2025-25187	Cross-site Scripting in Goto Anything allows arbitrary code execution in Joplin	Joplin is a free, open source note taking and to-do application, which can handle a large number of notes organised into notebooks. This vulnerability is caused by adding note titles to the document using React's `dangerouslySetInnerHTML`, without first escaping HTML entities. Joplin lacks a Content-Security-Policy with a restrictive `script-src`. This allows arbitrary JavaScript execution via inline `onclick`/`onload` event handlers in unsanitized HTML. Additionally, Joplin's main window is created with `nodeIntegration` set to `true`, allowing arbitrary JavaScript execution to result in arbitrary code execution. Anyone who 1) receives notes from unknown sources	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and 2) uses <kbd>ctrl</kbd>-<kbd>p</kbd> to search is impacted. This issue has been addressed in version 3.1.24 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-27092	Path Traversal Vulnerability in GHOSTS Photo Retrieval Endpoint	GHOSTS is an open source user simulation framework for cyber experimentation, simulation, training, and exercise. A path traversal vulnerability was discovered in GHOSTS version 8.0.0.0 that allows an attacker to access files outside of the intended directory through the photo retrieval endpoint. The vulnerability exists in the /api/npcs/{id}/photo endpoint, which is designed to serve profile photos for NPCs (Non-Player Characters) but fails to properly validate and sanitize file paths. When an NPC is created with a specially crafted photoLink value containing path traversal sequences (../, ..\, etc.), the application processes these sequences without proper sanitization. This allows an attacker to traverse directory structures and access files outside of the intended photo directory, potentially exposing sensitive system files. The vulnerability is particularly severe	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		because it allows reading arbitrary files from the server's filesystem with the permissions of the web application process, which could include configuration files, credentials, or other sensitive data. This issue has been addressed in version 8.2.7.90 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-27137	Dependency-Track vulnerable to local file inclusion via custom notification templates	Dependency-Track is a component analysis platform that allows organizations to identify and reduce risk in the software supply chain. Dependency-Track allows users with the `SYSTEM_CONFIGURATION` permission to customize notification templates. Templates are evaluated using the Pebble template engine. Pebble supports an `include` tag, which allows template authors to include the content of arbitrary files upon evaluation. Prior to version 4.12.6, users of Dependency-Track with the `SYSTEM_CONFIGURATION` permission can abuse the `include` tag by crafting notification templates that `include` sensitive local files, such as `/etc/passwd` or `/proc/1/environ`. By configuring such a template for a notification rule (aka "Alert"), and having it send notifications to a destination controlled	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by the actor, sensitive information may be leaked. The issue has been fixed in Dependency-Track 4.12.6. In fixed versions, the `include` tag can no longer be used. Usage of the tag will cause template evaluation to fail. As a workaround, avoid assigning the `SYSTEM_CONFIGURATION` permission to untrusted users. The `SYSTEM_CONFIGURATION` permission per default is only granted to members of the `Administrators` team. Assigning this permission to non-administrative users or teams is a security risk in itself, and highly discouraged.		

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-11956	Pimcore customer-data-framework list sql injection	A vulnerability, which was classified as critical, has been found in Pimcore customer-data-framework up to 4.2.0. Affected by this issue is some unknown functionality of the file /admin/customermanagementframework/customers/list. The manipulation of the argument filterDefinition/filter leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.2.1 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-13478	LTL Freight Quotes – TForce Edition <= 3.6.4 - Unauthenticated SQL Injection	The LTL Freight Quotes – TForce Edition plugin for WordPress is vulnerable to SQL Injection via the 'dropship_edit_id' and 'edit_id' parameters in all versions up to, and including, 3.6.4 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-2024-13479	LTL Freight Quotes – SEFL Edition <= 3.2.4 - Unauthenticated SQL Injection	The LTL Freight Quotes – SEFL Edition plugin for WordPress is vulnerable to SQL Injection via the 'dropship_edit_id' and 'edit_id' parameters in all versions up to, and including, 3.2.4 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-2024-13481	LTL Freight Quotes – R+L Carriers Edition <= 3.3.4 - Unauthenticated SQL Injection	The LTL Freight Quotes – R+L Carriers Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id'	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and 'dropship_edit_id' parameters in all versions up to, and including, 3.3.4 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.		
CVE-2024-13483	LTL Freight Quotes – SAIA Edition <= 2.2.10 - Unauthenticated SQL Injection	The LTL Freight Quotes – SAIA Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 2.2.10 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-2024-13485	LTL Freight Quotes – ABF Freight Edition <= 3.3.7 - Unauthenticated SQL Injection	The LTL Freight Quotes – ABF Freight Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 3.3.7 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-2024-13488	LTL Freight Quotes – Estes Edition <= 3.3.7 - Unauthenticated SQL Injection	The LTL Freight Quotes – Estes Edition plugin for WordPress is vulnerable to SQL Injection via the 'dropship_edit_id' and 'edit_id' parameters in all versions up to, and including, 3.3.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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.		
CVE-2024-13489	LTL Freight Quotes – Old Dominion Edition <= 4.2.10 - Unauthenticated SQL Injection	The LTL Freight Quotes – Old Dominion Edition plugin for WordPress is vulnerable to SQL Injection via the 'edit_id' and 'dropship_edit_id' parameters in all versions up to, and including, 4.2.10 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-2024-54145	Cacti has a SQL Injection vulnerability when request automation devices	Cacti is an open source performance and fault management framework. Cacti has a SQL injection vulnerability in the get_discovery_results function of automation_devices.php using the network parameter. This vulnerability is fixed in 1.2.29.	Patched by core rule	Y
CVE-2024-54146	Cacti has a SQL Injection vulnerability when view host template	Cacti is an open source performance and fault management framework. Cacti has a SQL injection vulnerability in the template function of host_templates.php using the graph_template parameter. This vulnerability is fixed in 1.2.29.	Patched by core rule	Y
CVE-2025-0786	ESAFENET CDG appDetail.jsp sql injection	A vulnerability was found in ESAFENET CDG V5. It has been classified as critical. Affected is an unknown function of the file /appDetail.jsp. The manipulation of the argument flowId leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-0788	ESAFENET CDG content_top.jsp sql injection	A vulnerability was found in ESAFENET CDG V5. It has been rated as critical. Affected by this issue is some unknown functionality of the file /content_top.jsp. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0789	ESAFENET CDG doneDetail.jsp sql injection	A vulnerability classified as critical has been found in ESAFENET CDG V5. This affects an unknown part of the file /doneDetail.jsp. The manipulation of the argument flowId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0791	ESAFENET CDG sdDoneDetail.jsp sql injection	A vulnerability, which was classified as critical, has been found in ESAFENET CDG V5. This issue affects some unknown processing of the file /sdDoneDetail.jsp. The manipulation of the argument flowId leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0792	ESAFENET CDG sdTodoDetail.jsp sql injection	A vulnerability, which was classified as critical, was found in ESAFENET CDG V5. Affected is an unknown function of the file /sdTodoDetail.jsp. The manipulation of the argument flowId leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0793	ESAFENET CDG	A vulnerability has been	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	todoDetail.jsp sql injection	found in ESAFENET CDG V5 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /todoDetail.jsp. The manipulation of the argument flowId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	rule	
CVE-2025-0803	Codezips Gym Management System submit_plan_new.php sql injection	A vulnerability, which was classified as critical, has been found in Codezips Gym Management System 1.0. Affected by this issue is some unknown functionality of the file /dashboard/admin/submit_plan_new.php. The manipulation of the argument planid 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-2025-0846	1000 Projects Employee Task Management System AdminLogin.php sql injection	A vulnerability was found in 1000 Projects Employee Task Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/AdminLogin.php. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0847	1000 Projects Employee Task Management System Login index.php sql injection	A vulnerability was found in 1000 Projects Employee Task Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /index.php of the component Login. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0872	itsourcecode Tailoring Management System addpayment.php sql injection	A vulnerability classified as critical has been found in itsourcecode Tailoring Management System 1.0. Affected is an unknown function of the file /addpayment.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument id/amount/desc/inccat leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0873	itsourcecode Tailoring Management System customeredit.php sql injection	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /customeredit.php. The manipulation of the argument id/address/fullname/phonenumber/email/city/comment leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0874	code-projects Simple Plugins Car Rental Management approve.php sql injection	A vulnerability, which was classified as critical, has been found in code-projects Simple Plugins Car Rental Management 1.0. Affected by this issue is some unknown functionality of the file /admin/approve.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0881	Codezips Gym Management System saveroutine.php sql injection	A vulnerability was found in Codezips Gym Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /dashboard/admin/saveroutine.php. The manipulation of the argument rname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0882	code-projects Chat System addnewmember.php sql injection	A vulnerability was found in code-projects Chat System up to 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /user/addnewmember.php. The manipulation of the argument user leads to sql injection. The attack can be launched remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been disclosed to the public and may be used.		
CVE-2025-0934	code-projects Job Recruitment _call_job_search_ajax.php sql injection	A vulnerability was found in code-projects Job Recruitment 1.0. It has been classified as problematic. This affects an unknown part of the file /parse/_call_job_search_ajax.php. The manipulation of the argument n leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0943	itsourcecode Tailoring Management System deldoc.php sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file deldoc.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0944	itsourcecode Tailoring Management System customerview.php sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file customerview.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0945	itsourcecode Tailoring Management System typedelete.php sql injection	A vulnerability classified as critical has been found in itsourcecode Tailoring Management System 1.0. Affected is an unknown function of the file typedelete.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0946	itsourcecode Tailoring Management System templatedelete.php sql injection	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. Affected by this vulnerability is an unknown functionality of the file templatedelete.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. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0947	itsourcecode Tailoring Management System expview.php sql injection	A vulnerability, which was classified as critical, has been found in itsourcecode Tailoring Management System 1.0. Affected by this issue is some unknown functionality of the file expview.php. The manipulation of the argument expid 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-2025-0948	itsourcecode Tailoring Management System incview.php sql injection	A vulnerability, which was classified as critical, was found in itsourcecode Tailoring Management System 1.0. This affects an unknown part of the file incview.php. The manipulation of the argument incid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0949	itsourcecode Tailoring Management System partview.php sql injection	A vulnerability has been found in itsourcecode Tailoring Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file partview.php. The manipulation of the argument typeid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0950	itsourcecode Tailoring Management System staffview.php sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. This issue affects some unknown processing of the file staffview.php. The manipulation of the argument staffid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0967	code-projects Chat System add_chatroom.php sql injection	A vulnerability was found in code-projects Chat System 1.0 and classified as critical. This issue affects some	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown processing of the file /user/add_chatroom.php. The manipulation of the argument chatname/chatpass leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1023	SQL Injection in ChurchCRM newCountName Parameter via EditEventTypes.php	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to execute arbitrary SQL queries by exploiting a time-based blind SQL Injection vulnerability in the EditEventTypes functionality . The newCountName parameter is directly concatenated into an SQL query without proper sanitization, allowing an attacker to manipulate database queries and execute arbitrary commands, potentially leading to data exfiltration, modification, or deletion.	Patched by core rule	Y
CVE-2025-1116	Dreamvention Live AJAX Search Free live_search.searchresults search sql injection	A vulnerability, which was classified as critical, has been found in Dreamvention Live AJAX Search Free up to 1.0.6 on OpenCart. Affected by this issue is the function searchresults/search of the file /?route=extension/live_search/module/live_search.searchresults. The manipulation of the argument keyword 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-2025-1117	CoinRemitter sql injection	A vulnerability, which was classified as critical, was found in CoinRemitter 0.0.1/0.0.2 on OpenCart. This affects an unknown part. The manipulation of the argument coin leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 0.0.3 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-1132	SQL Injection in ChurchCRM EN_tyid Parameter via	A time-based blind SQL Injection vulnerability exists in the ChurchCRM 5.13.0	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	EditEventAttendees.php	and prior EditEventAttendees.php within the EN_tyid parameter. The parameter is directly inserted into an SQL query without proper sanitization, allowing attackers to inject malicious SQL commands. Please note that the vulnerability requires Administrator permissions. This flaw can potentially allow attackers to delay the response, indicating the presence of an SQL injection vulnerability. While it is a time-based blind injection, it can be exploited to gain insights into the underlying database, and with further exploitation, sensitive data could be retrieved.		
CVE-2025-1133	SQL Injection in ChurchCRM EID Parameter via EditEventAttendees.php	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to execute arbitrary SQL queries by exploiting a boolean-based blind SQL Injection vulnerability in the EditEventAttendees functionality. The EID parameter is directly concatenated into an SQL query without proper sanitization, making it susceptible to SQL injection attacks. An attacker can manipulate the query, potentially leading to data exfiltration, modification, or deletion. Please note that this vulnerability requires Administrator privileges.	Patched by core rule	Y
CVE-2025-1134	SQL Injection in ChurchCRM CurrentFundraiser Parameter via DonatedItemEditor.php	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to execute arbitrary SQL queries by exploiting a boolean-based and time-based blind SQL Injection vulnerability in the DonatedItemEditor functionality. The CurrentFundraiser parameter is directly concatenated into an SQL query without sufficient sanitization, allowing an attacker to manipulate database queries and execute arbitrary commands, potentially leading to data exfiltration, modification, or deletion. Please note that this vulnerability requires		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Administrator privileges.		
CVE-2025-1135	SQL Injection in ChurchCRM CurrentFundraiser Parameter via BatchWinnerEntry.php	A vulnerability exists in ChurchCRM 5.13.0. and prior that allows an attacker to execute arbitrary SQL queries by exploiting a boolean-based and time-based blind SQL Injection vulnerability in the BatchWinnerEntry functionality. The CurrentFundraiser parameter is directly concatenated into an SQL query without sufficient sanitization, allowing an attacker to manipulate database queries and execute arbitrary commands, potentially leading to data exfiltration, modification, or deletion. Please note the vulnerability requires Administrator privileges.	Patched by core rule	Y
CVE-2025-1154	xxyopen Novel books sql injection	A vulnerability, which was classified as critical, has been found in xxyopen Novel up to 3.4.1. Affected by this issue is some unknown functionality of the file /api/front/search/books. The manipulation of the argument sort leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-1158	ESAFENET CDG addPolicyToSafetyGroup.jsp sql injection	A vulnerability was found in ESAFENET CDG 5.6.3.154.205_20250114. It has been classified as critical. Affected is an unknown function of the file addPolicyToSafetyGroup.jsp. The manipulation of the argument safetyGroupId leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1162	code-projects Job Recruitment load_user-profile.php sql injection	A vulnerability classified as critical has been found in code-projects Job Recruitment 1.0. This affects an unknown part of the file /_parse/load_user-profile.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument userhash leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1172	1000 Projects Bookstore Management System addtocart.php sql injection	A vulnerability, which was classified as critical, has been found in 1000 Projects Bookstore Management System 1.0. Affected by this issue is some unknown functionality of the file addtocart.php. The manipulation of the argument bcid 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-2025-1173	1000 Projects Bookstore Management System process_users_del.php sql injection	A vulnerability, which was classified as critical, was found in 1000 Projects Bookstore Management System 1.0. This affects an unknown part of the file process_users_del.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely.	Patched by core rule	Y
CVE-2025-1184	pihome-shc PiHome ajax.php sql injection	A vulnerability was found in pihome-shc PiHome 1.77 and classified as critical. Affected by this issue is some unknown functionality of the file /ajax.php?Ajax=GetModal_MQTTEdit. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1185	pihome-shc PiHome ajax.php sql injection	A vulnerability was found in pihome-shc PiHome 2.0. It has been classified as critical. This affects an unknown part of the file /ajax.php?Ajax=GetModal_Sensor_Graph. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1188	Codezips Gym Management System updateroutine.php sql injection	A vulnerability, which was classified as critical, has been found in Codezips Gym Management System 1.0. Affected by this issue is some unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/dashboard/admin/updateroutine.php. The manipulation of the argument tid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1189	1000 Projects Attendance Tracking Management System chart1.php sql injection	A vulnerability, which was classified as critical, was found in 1000 Projects Attendance Tracking Management System 1.0. This affects an unknown part of the file /admin/chart1.php. The manipulation of the argument course_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1191	SourceCodester Multi Restaurant Table Reservation System approve-reject.php sql injection	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0 and classified as critical. This issue affects some unknown processing of the file /dashboard/approve-reject.php. The manipulation of the argument breject_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1192	SourceCodester Multi Restaurant Table Reservation System select-menu.php sql injection	A vulnerability was found in SourceCodester Multi Restaurant Table Reservation System 1.0. It has been classified as critical. Affected is an unknown function of the file select-menu.php. The manipulation of the argument table leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1197	code-projects Real Estate Property Management System load_user-profile.php sql injection	A vulnerability has been found in code-projects Real Estate Property Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /_parse/load_user-profile.php. The manipulation of the argument userhash leads to sql injection. The attack can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1199	SourceCodester Best Church Management Software role_crud.php sql injection	A vulnerability was found in SourceCodester Best Church Management Software 1.1. It has been classified as critical. This affects an unknown part of the file /admin/app/role_crud.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1200	SourceCodester Best Church Management Software slider_crud.php sql injection	A vulnerability was found in SourceCodester Best Church Management Software 1.1. It has been declared as critical. This vulnerability affects unknown code of the file /admin/app/slider_crud.php. The manipulation of the argument del_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1201	SourceCodester Best Church Management Software profile_crud.php sql injection	A vulnerability was found in SourceCodester Best Church Management Software 1.1. It has been rated as critical. This issue affects some unknown processing of the file /admin/app/profile_crud.php. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Multiple parameters might be affected.	Patched by core rule	Y
CVE-2025-1202	SourceCodester Best Church Management Software edit_slider.php sql injection	A vulnerability classified as critical has been found in SourceCodester Best Church Management Software 1.1. Affected is an unknown function of the file /admin/edit_slider.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1206	Codezips Gym Management System viewdetailroutine.php sql injection	A vulnerability was found in Codezips Gym Management System 1.0. It has been classified as critical. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects an unknown part of the file /dashboard/admin/viewdetailroutine.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1210	code-projects Wazifa System control.php sql injection	A vulnerability classified as critical was found in code-projects Wazifa System 1.0. Affected by this vulnerability is an unknown functionality of the file /controllers/control.php. The manipulation of the argument to leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1216	ywoa OaNoticeMapper.xml selectNoticeList sql injection	A vulnerability, which was classified as critical, has been found in ywoa up to 2024.07.03. This issue affects the function selectNoticeList of the file com/cloudweb/oa/mapper/xml/OaNoticeMapper.xml. The manipulation of the argument sort leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-1224	ywoa UserMapper.xml listNameBySql sql injection	A vulnerability classified as critical was found in ywoa up to 2024.07.03. This vulnerability affects the function listNameBySql of the file com/cloudweb/oa/mapper/xml/UserMapper.xml. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-1227	ywoa AddressDao.xml selectList sql injection	A vulnerability was found in ywoa up to 2024.07.03. It has been rated as critical. This issue affects the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function selectList of the file com/cloudweb/oa/mapper/xml/AddressDao.xml. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.		
CVE-2025-1374	code-projects Real Estate Property Management System search.php sql injection	A vulnerability classified as critical has been found in code-projects Real Estate Property Management System 1.0. This affects an unknown part of the file /search.php. The manipulation of the argument StateName/CityName/AreaName/CatId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1379	code-projects Real Estate Property Management System CustomerReport.php sql injection	A vulnerability has been found in code-projects Real Estate Property Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /Admin/CustomerReport.php. The manipulation of the argument city leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1381	code-projects Real Estate Property Management System ajax_city.php sql injection	A vulnerability was found in code-projects Real Estate Property Management System 1.0. It has been classified as critical. This affects an unknown part of the file /ajax_city.php. The manipulation of the argument CityName leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1464	Baiyi Cloud Asset Management System admin.house.collect.php sql injection	A vulnerability, which was classified as critical, has been found in Baiyi Cloud Asset Management System up to 20250204. 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
		/wuser/admin.house.collect.php. The manipulation of the argument project_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1535	Baiyi Cloud Asset Management System admin.ticket.close.php sql injection	A vulnerability was found in Baiyi Cloud Asset Management System 8.142.100.161. It has been classified as critical. This affects an unknown part of the file /wuser/admin.ticket.close.php. The manipulation of the argument ticket_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1544	dingfanzu CMS loadShopInfo.php sql injection	A vulnerability, which was classified as critical, was found in dingfanzu CMS up to 20250210. Affected is an unknown function of the file /ajax/loadShopInfo.php. The manipulation of the argument shopId leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1576	code-projects Real Estate Property Management System ajax_state.php sql injection	A vulnerability classified as critical was found in code-projects Real Estate Property Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax_state.php. The manipulation of the argument StateName as part of String leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1578	PHPGurukul Online Shopping Portal search-result.php sql injection	A vulnerability, which was classified as critical, was found in PHPGurukul Online Shopping Portal 2.1. This affects an unknown part of the file /search-result.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument product leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1580	PHPGurukul Nipah Virus Testing Management System search-report-result.php sql injection	A vulnerability was found in PHPGurukul Nipah Virus Testing Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /search-report-result.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting parameter names to be affected.	Patched by core rule	Y
CVE-2025-1581	PHPGurukul Online Nurse Hiring System book-nurse.php sql injection	A vulnerability was found in PHPGurukul Online Nurse Hiring System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /book-nurse.php?bookid=1. The manipulation of the argument contactname leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1582	PHPGurukul Online Nurse Hiring System all-request.php sql injection	A vulnerability was found in PHPGurukul Online Nurse Hiring System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/all-request.php. The manipulation of the argument viewid 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-2025-1583	PHPGurukul Online Nurse Hiring System search-report-details.php sql injection	A vulnerability classified as critical has been found in PHPGurukul Online Nurse Hiring System 1.0. This affects an unknown part of the file /admin/search-report-details.php. The manipulation of the argument searchinput leads to sql injection. It is possible to initiate the attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1596	SourceCodester Best Church Management Software fpassword.php sql injection	A vulnerability was found in SourceCodester Best Church Management Software 1.0 and classified as critical. This issue affects some unknown processing of the file /fpassword.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1640	Benner ModernaNet JS_CarregaCombo sql injection	A vulnerability was found in Benner ModernaNet up to 1.1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /Home/JS_CarregaCombo?formName=DADOS_PESSOAIS_PLANO&additionalCondition=&insideParameters=&elementToReturn=DADOS_PESSOAIS_PLANO&ordenarPelaDescricao=true&direcaoOrdenacao=asc&_=1739290047295. The manipulation leads to sql injection. The attack may be launched remotely. Upgrading to version 1.1.1 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-1641	Benner ModernaNet GetHorariosDoDia sql injection	A vulnerability was found in Benner ModernaNet up to 1.1.0. It has been classified as critical. This affects an unknown part of the file /AGE0000700/GetHorariosDoDia?idespec=0&idproced=1103&data=2025-02-25+19%3A25&agserv=0&convenio=1&localatend=1&idplano=5&pesfis=01&idprofissional=0&target=.horarios--dia--d0&_=1739371223797. The manipulation leads to sql injection. It is possible to initiate the attack remotely. Upgrading to version 1.1.1 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-22208	Extension - joomsky.com - SQL injection in JS jobs component version 1.1.5 - 1.4.3 for Joomla	A SQL injection vulnerability in the JS Jobs plugin versions 1.1.5-1.4.3 for Joomla allows authenticated attackers	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		(administrator) to execute arbitrary SQL commands via the 'filter_email' parameter in the GDPR Erase Data Request search feature.		
CVE-2025-22209	Extension - joomsky.com - SQL injection in JS jobs component version 1.1.5 - 1.4.3 for Joomla	A SQL injection vulnerability in the JS Jobs plugin versions 1.1.5-1.4.3 for Joomla allows authenticated attackers (administrator) to execute arbitrary SQL commands via the 'searchpaymentstatus' parameter in the Employer Payment History search feature.	Patched by core rule	Y
CVE-2025-22210	Extension - hikashop.com - SQL injection in Hikashop component version 3.3.0 - 5.1.4 for Joomla	A SQL injection vulnerability in the Hikashop component versions 3.3.0-5.1.4 for Joomla allows authenticated attackers (administrator) to execute arbitrary SQL commands in the category management area in backend.	Patched by core rule	Y
CVE-2025-22211	Extension - webdesigner-profi.de - SQL injection in JoomShopping component version 1.0.0 - 5.5.5 for Joomla	A SQL injection vulnerability in the JoomShopping component versions 1.0.0-1.4.3 for Joomla allows authenticated attackers (administrator) to execute arbitrary SQL commands in the country management area in backend.	Patched by core rule	Y
CVE-2025-24368	Cacti has a SQL Injection vulnerability when using tree rules through Automation API	Cacti is an open source performance and fault management framework. Some of the data stored in automation_tree_rules.php is not thoroughly checked and is used to concatenate the SQL statement in build_rule_item_filter() function from lib/api_automation.php, resulting in SQL injection. This vulnerability is fixed in 1.2.29.	Patched by core rule	Y
CVE-2025-24612	WordPress Shipping for Nova Poshta plugin <= 1.19.6 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MORKVA Shipping for Nova Poshta allows SQL Injection. This issue affects Shipping for Nova Poshta: from n/a through 1.19.6.	Patched by core rule	Y
CVE-2025-24664	WordPress LTL Freight Quotes Plugin <= 5.0.20 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eniture Technology LTL Freight Quotes – Worldwide Express Edition allows SQL Injection. This issue affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		LTL Freight Quotes – Worldwide Express Edition: from n/a through 5.0.20.		
CVE-2025-24665	WordPress Small Package Quotes Plugin <= 2.4.8 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eniture Technology Small Package Quotes – Unishippers Edition allows SQL Injection. This issue affects Small Package Quotes – Unishippers Edition: from n/a through 2.4.8.	Patched by core rule	Y
CVE-2025-24667	WordPress Small Package Quotes Plugin <= 5.2.17 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eniture Technology Small Package Quotes – Worldwide Express Edition allows SQL Injection. This issue affects Small Package Quotes – Worldwide Express Edition: from n/a through 5.2.17.	Patched by core rule	Y
CVE-2025-24793	Snowflake Connector for Python has an SQL Injection in write_pandas	The Snowflake Connector for Python provides an interface for developing Python applications that can connect to Snowflake and perform all standard operations. Snowflake discovered and remediated a vulnerability in the Snowflake Connector for Python. A function from the snowflake.connector.pandas_tools module is vulnerable to SQL injection. This vulnerability affects versions 2.2.5 through 3.13.0. Snowflake fixed the issue in version 3.13.1.	Patched by core rule	Y
CVE-2025-24901	SQL Injection endpoint 'deletar_permissao.php' parameter 'c', 'a', 'r' in WeGIA	WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `deletar_permissao.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-24902	SQL Injection endpoint 'salvar_cargo.php'	WeGIA is a Web Manager for Charitable Institutions. A	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	parameter 'id_cargo' in WeGIA	SQL Injection vulnerability was discovered in the WeGIA application, `salvar_cargo.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-24905	SQL Injection endpoint 'get_codigobarras_cobranca.php' parameter 'codigo' in WeGIA	WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `get_codigobarras_cobranca.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-24906	SQL Injection endpoint 'get_detalhes_cobranca.php' parameter 'codigo' in WeGIA	WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `get_detalhes_cobranca.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-24957	SQL Injection endpoint 'get_detalhes_socio.php' parameter 'id_socio' in WeGIA	WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `get_detalhes_socio.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		are no known workarounds for this vulnerability.		
CVE-2025-24958	SQL Injection endpoint 'salvar_tag.php' parameter 'id_tag' in WeGIA	WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `salvar_tag.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-25116	WordPress Link to URL / Post plugin <=1.3 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in sudipto Link to URL / Post allows Blind SQL Injection. This issue affects Link to URL / Post: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-25151	WordPress uListing Plugin <= 2.1.6 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes uListing allows SQL Injection. This issue affects uListing: from n/a through 2.1.6.	Patched by core rule	Y
CVE-2025-26520	N/A	Cacti through 1.2.29 allows SQL injection in the template function in host_templates.php via the graph_template parameter. NOTE: this issue exists because of an incomplete fix for CVE-2024-54146.	Patched by core rule	Y
CVE-2025-26605	SQL Injection endpoint 'deletar_cargo.php' parameter 'id_cargo' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `deletar_cargo.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-26606	SQL Injection endpoint 'informacao_adicional.ph	WeGIA is an open source Web Manager for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	p' parameter 'id_descricao' in WeGIA	Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `informacao_adicional.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-26607	SQL Injection endpoint 'documento_excluir.php' parameter 'id_funcionario' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `documento_excluir.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-26608	SQL Injection endpoint 'dependente_docdependente.php' parameter 'id_dependente', 'id_doc' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `dependente_docdependente.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-26609	SQL Injection endpoint 'familiar_docfamiliar.php' parameter 'id_dependente', 'id_doc' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		`familiar_docfamiliar.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-26610	SQL Injection endpoint 'restaurar_produto_desocultar.php' parameter 'id_produto' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `restaurar_produto_desocultar.php` endpoint. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-26611	SQL Injection endpoint 'remover_produto.php' parameter 'id_produto' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `remover_produto.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-26612	SQL Injection endpoint 'adicionar_almoxarife.php' parameter 'id_almoxarifado', 'id_funcionario' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `adicionar_almoxarife.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unauthorized access to sensitive information. This issue has been addressed in version 3.2.13 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-26614	SQL Injection endpoint 'deletar_documento.php' parameter 'id_cargo' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `deletar_documento.php` endpoint. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-26617	SQL Injection endpoint 'historico_paciente.php' parameter 'id_fichamedica' in WeGIA	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A SQL Injection vulnerability was discovered in the WeGIA application, `historico_paciente.php` endpoint. This vulnerability could allow an attacker to execute arbitrary SQL queries, allowing unauthorized access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-26755	WordPress WP Airbnb Review Slider Plugin <= 3.9 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in jgwhite33 WP Airbnb Review Slider allows Blind SQL Injection. This issue affects WP Airbnb Review Slider: from n/a through 3.9.	Patched by core rule	Y
CVE-2025-26794	N/A	Exim 4.98 before 4.98.1, when SQLite hints and ETRN serialization are used, allows remote SQL injection.	Patched by core rule	Y
CVE-2025-26915	WordPress Wishlist Plugin <= 1.0.41 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		PickPlugins Wishlist allows SQL Injection. This issue affects Wishlist: from n/a through 1.0.41.		
CVE-2025-26943	WordPress Easy Quotes plugin <= 1.2.2 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jürgen Müller Easy Quotes allows Blind SQL Injection. This issue affects Easy Quotes: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-26946	WordPress WP Yelp Review Slider Plugin <= 8.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in jgwhite33 WP Yelp Review Slider allows Blind SQL Injection. This issue affects WP Yelp Review Slider: from n/a through 8.1.	Patched by core rule	Y
CVE-2025-26971	WordPress Poll Maker <= 5.6.5 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ays-pro Poll Maker allows Blind SQL Injection. This issue affects Poll Maker: from n/a through 5.6.5.	Patched by core rule	Y
CVE-2025-26974	WordPress WP Multi Store Locator plugin <= 2.5.1 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPExperts.io WP Multi Store Locator allows Blind SQL Injection. This issue affects WP Multi Store Locator: from n/a through 2.5.1.	Patched by core rule	Y
CVE-2025-27096	SQL Injection endpoint 'html/personalizacao_upload.php' parameter 'id_campo' in WeGIA	WeGIA is a Web Manager for Institutions with a focus on Portuguese language. A SQL Injection vulnerability was discovered in the WeGIA application, personalizacao_upload.php endpoint. This vulnerability allow an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. This issue has been addressed in version 3.2.14 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-27133	WeGIA has SQL Injection endpoint at 'dao/pet/adicionar_tipo_exame.php' parameter 'tipo_exame'	WeGIA is a Web manager for charitable institutions. A SQL Injection vulnerability was discovered in the WeGIA application prior to version 3.2.15 at the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		`adicionar_tipo_exame.php` endpoint. This vulnerability allows an authorized attacker to execute arbitrary SQL queries, allowing access to sensitive information. Version 3.2.15 contains a patch for the issue.		
CVE-2025-27135	RAGFlow SQL Injection vulnerability	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. Versions 0.15.1 and prior are vulnerable to SQL injection. The ExeSQL component extracts the SQL statement from the input and sends it directly to the database query. As of time of publication, no patched version is available.	Patched by core rule	Y
CVE-2025-27297	WordPress Bravo Search & Replace Plugin <= 1.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in guelben Bravo Search & Replace allows Blind SQL Injection. This issue affects Bravo Search & Replace: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-27312	WordPress WP Sitemap plugin <= 1.0 - SQL Injection vulnerability	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jenst WP Sitemap allows SQL Injection. This issue affects WP Sitemap: from n/a through 1.0.	Patched by core rule	Y

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-25066	N/A	RSA Authentication Manager before 8.7 SP2 Patch 1 allows XML External Entity (XXE) attacks via a license file, resulting in attacker-controlled files being stored on the product's server. Data exfiltration cannot occur.	Patched by core rule	Y
CVE-2025-1225	ywoa WXCallBack Interface XMLParse.java extract xml external entity reference	A vulnerability, which was classified as problematic, has been found in ywoa up to 2024.07.03. This issue affects the function extract of the file c-main/src/main/java/com/redmoon/weixin/aes/XMLParse.java of the component WXCallBack Interface. The manipulation leads to xml external entity reference. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2024.07.04 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-10222	SVG Support <= 2.5.10 - Authenticated (Author+) Stored Cross-Site Scripting via SVG File Upload	The SVG Support plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.5.10 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file. By default, this can only be exploited by administrators, but the ability to upload SVG files can be extended to authors.	Patched by core rule	Y
CVE-2024-10383	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitLab VSCode Fork	An issue has been discovered in the gitlab-web-ide-vscode-fork component distributed over CDN affecting all versions prior to 1.89.1-1.0.0-dev-20241118094343and used by all versions of GitLab CE/EE starting from 15.11 prior to 17.3 and which also temporarily affected versions 17.4, 17.5 and 17.6, where a XSS attack was possible when loading .ipynb files in the web IDE	Patched by core rule	Y
CVE-2024-10649	Unauthenticated File Upload in wandb/openui	wandb/openui latest commit c945bb859979659add5f490a874140ad17c56a5d contains a vulnerability where unauthenticated endpoints allow file uploads and downloads from an AWS S3 bucket. This can lead to multiple security issues including denial of service, stored XSS, and information disclosure. The affected endpoints are '/v1/share/{id:str}' for uploading and '/v1/share/{id:str}' for downloading JSON files. The lack of authentication allows any user to upload and overwrite files, potentially causing the S3 bucket to run out of space, injecting malicious scripts, and accessing sensitive information.	Patched by core rule	Y
CVE-2024-11623	Stored XSS in authentik	Authentik project is vulnerable to Stored XSS	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attacks through uploading crafted SVG files that are used as application icons. This action could only be performed by an authenticated admin user. The issue was fixed in 2024.10.4 release.		
CVE-2024-11831	Npm-serialize-javascript: cross-site scripting (xss) in serialize-javascript	A flaw was found in npm-serialize-javascript. The vulnerability occurs because the serialize-javascript module does not properly sanitize certain inputs, such as regex or other JavaScript object types, allowing an attacker to inject malicious code. This code could be executed when deserialized by a web browser, causing Cross-site scripting (XSS) attacks. This issue is critical in environments where serialized data is sent to web clients, potentially compromising the security of the website or web application using this package.	Patched by core rule	Y
CVE-2024-11954	Pimcore Search Document cross site scripting	A vulnerability classified as problematic was found in Pimcore 11.4.2. Affected by this vulnerability is an unknown functionality of the component Search Document. The manipulation leads to basic cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2024-53266	Cross-site Scripting (XSS) via topic titles when CSP disabled in Discourse	Discourse is an open source platform for community discussion. In affected versions with some combinations of plugins, and with CSP disabled, activity streams in the user's profile page may be vulnerable to XSS. This has been patched in the latest version of Discourse core. Users are advised to upgrade. Users unable to upgrade should ensure CSP is enabled.	Patched by core rule	Y
CVE-2024-54160	N/A	dashboards-reporting (aka Dashboards Reports) before 2.19.0.0, as shipped in OpenSearch before 2.19, allows XSS because Markdown is not sanitized when previewing a header or footer.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-0376	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitLab	An XSS vulnerability exists in GitLab CE/EE affecting all versions from 13.3 prior to 17.6.5, 17.7 prior to 17.7.4 and 17.8 prior to 17.8.2 that allows an attacker to execute unauthorized actions via a change page.	Patched by core rule	Y
CVE-2025-0785	ESAFENET CDG SysConfig.jsp cross site scripting	A vulnerability was found in ESAFENET CDG V5 and classified as problematic. This issue affects some unknown processing of the file /SysConfig.jsp. The manipulation of the argument help leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0787	ESAFENET CDG appDetail.jsp cross site scripting	A vulnerability was found in ESAFENET CDG V5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /appDetail.jsp. The manipulation of the argument curpage leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0790	ESAFENET CDG doneDetail.jsp cross site scripting	A vulnerability classified as problematic was found in ESAFENET CDG V5. This vulnerability affects unknown code of the file /doneDetail.jsp. The manipulation of the argument curpage leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0794	ESAFENET CDG todoDetail.jsp cross site scripting	A vulnerability was found in ESAFENET CDG V5 and classified as problematic. Affected by this issue is some unknown functionality of the file /todoDetail.jsp. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument curpage leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-0795	ESAFENET CDG todolistjump.jsp cross site scripting	A vulnerability was found in ESAFENET CDG V5. It has been classified as problematic. This affects an unknown part of the file /todolistjump.jsp. The manipulation of the argument flowId leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-0806	code-projects Job Recruitment _call_job_search_ajax.php cross site scripting	A vulnerability was found in code-projects Job Recruitment 1.0. It has been rated as problematic. This issue affects some unknown processing of the file _call_job_search_ajax.php. The manipulation of the argument job_type leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0871	Maybecms Add Article index.php cross site scripting	A vulnerability classified as problematic has been found in Maybecms 1.2. This affects an unknown part of the file /mb/admin/index.php?u=article-edit of the component Add Article. The manipulation of the argument data_info[content] leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-0961	code-projects Job Recruitment load_job-details.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Job Recruitment 1.0. Affected by this issue is some unknown functionality of the file /_parse/load_job-details.php. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		business_stream_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-0972	Zenvia Movidesk New Ticket cross site scripting	A vulnerability classified as problematic has been found in Zenvia Movidesk up to 25.01.22. This affects an unknown part of the component New Ticket Handler. The manipulation of the argument subject leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 25.01.22.245a473c54 is able to address this issue. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2025-0981	Session Hijacking via Stored Cross-Site Scripting (XSS) in ChurchCRM Group Editor	A vulnerability exists in ChurchCRM 5.13.0 and prior that allows an attacker to hijack a user's session by exploiting a Stored Cross Site Scripting (XSS) vulnerability in the Group Editor page. This allows admin users to inject malicious JavaScript, which captures the session cookie of authenticated users. The cookie can then be sent to an external server, enabling session hijacking. It can also lead to information disclosure, as exposed session cookies can be used to impersonate users and gain unauthorised access to sensitive information.	Patched by core rule	Y
CVE-2025-1024	Session Hijacking via Reflected Cross-Site Scripting (XSS) in ChurchCRM EditEventAttendees.php EID Parameter	A vulnerability exists in ChurchCRM 5.13.0 that allows an attacker to execute arbitrary JavaScript in a victim's browser via Reflected Cross-Site Scripting (XSS) in the EditEventAttendees.php page. This requires Administration privileges and affects the EID parameter. The flaw allows an attacker to steal session cookies, perform actions on behalf of an authenticated user, and gain unauthorized access to the application.	Patched by core rule	Y
CVE-2025-1082	Mindskip xzs-mysql 学之思开源考试系统 Exam	A vulnerability classified as problematic has been found in Mindskip xzs-mysql 学之	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Edit edit cross site scripting	思开源考试系统 3.9.0. Affected is an unknown function of the file /api/admin/question/edit of the component Exam Edit Handler. The manipulation of the argument title/content leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-1114	newbee-mall Add Category Page save cross site scripting	A vulnerability classified as problematic has been found in newbee-mall 1.0. Affected is the function save of the file /admin/categories/save of the component Add Category Page. The manipulation of the argument categoryName leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. 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-2025-1155	Webkul QloApps Your Location Search stores cross site scripting	A vulnerability, which was classified as problematic, was found in Webkul QloApps 1.6.1. This affects an unknown part of the file /stores of the component Your Location Search. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. It is planned to remove this page in the long term.	Patched by core rule	Y
CVE-2025-1159	CampCodes School Management Software academic-calendar cross site scripting	A vulnerability was found in CampCodes School Management Software 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /academic-calendar. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1170	code-projects Real Estate Property Management System Category.php	A vulnerability classified as problematic has been found in code-projects Real Estate	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	Property Management System 1.0. Affected is an unknown function of the file /Admin/Category.php. The manipulation of the argument Desc leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1171	code-projects Real Estate Property Management System CustomerReport.php cross site scripting	A vulnerability classified as problematic was found in code-projects Real Estate Property Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /Admin/CustomerReport.php. The manipulation of the argument Address leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1174	1000 Projects Bookstore Management System Add Book Page process_book_add.php cross site scripting	A vulnerability has been found in 1000 Projects Bookstore Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file process_book_add.php of the component Add Book Page. The manipulation of the argument Book Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-1190	code-projects Job Recruitment load_user-profile.php cross site scripting	A vulnerability has been found in code-projects Job Recruitment 1.0 and classified as problematic. This vulnerability affects unknown code of the file /_parse/load_user-profile.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. Multiple parameters might be affected.	Patched by core rule	Y
CVE-2025-1195	code-projects Real Estate Property Management System EditCategory cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Real Estate Property Management System 1.0. This issue affects some unknown processing of the file /Admin/EditCategory.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument CategoryId leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1196	code-projects Real Estate Property Management System search.php cross site scripting	A vulnerability, which was classified as problematic, was found in code-projects Real Estate Property Management System 1.0. Affected is an unknown function of the file /search.php. The manipulation of the argument PropertyName leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2025-1208	code-projects Wazifa System Profile.php cross site scripting	A vulnerability was found in code-projects Wazifa System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /Profile.php. The manipulation of the argument postcontent leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1209	code-projects Wazifa System search_resualts.php searchuser cross site scripting	A vulnerability classified as problematic has been found in code-projects Wazifa System 1.0. Affected is the function searchuser of the file /search_resualts.php. The manipulation of the argument firstname/lastname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. There is a typo in the affected file name.	Patched by core rule	Y
CVE-2025-1213	pihome-shc PiHome index.php cross site scripting	A vulnerability was found in pihome-shc PiHome 1.77. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument $_SERVER['PHP_SELF'] leads to cross site scripting. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be launched remotely. The exploit has been disclosed to the public and may be used.		
CVE-2025-1332	FastCMS Template Menu menu cross site scripting	A vulnerability has been found in FastCMS up to 0.1.5 and classified as problematic. This vulnerability affects unknown code of the file /fastcms.html#/template/menu of the component Template Menu. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	Patched by core rule	Y
CVE-2025-1548	iteachyou Dreamer CMS edit cross site scripting	A vulnerability was found in iteachyou Dreamer CMS 4.1.3. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/archives/edit. The manipulation of the argument editorValue/answer/content leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-1577	code-projects Blood Bank System prostatus.php cross site scripting	A vulnerability, which was classified as problematic, has been found in code-projects Blood Bank System 1.0. Affected by this issue is some unknown functionality of the file /prostatus.php. The manipulation of the argument message leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1579	code-projects Blood Bank System user.php cross site scripting	A vulnerability was found in code-projects Blood Bank System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/user.php. The manipulation of the argument email leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.		
CVE-2025-1585	otale header.html OptionsService cross site scripting	A vulnerability, which was classified as problematic, has been found in otale tale up to 2.0.5. This issue affects the function OptionsService of the file src/main/resources/templates/themes/default/partial/header.html. The manipulation of the argument logo_url leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-1586	code-projects Blood Bank System A-.php cross site scripting	A vulnerability was found in code-projects Blood Bank System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /Blood/A-.php. The manipulation of the argument Bloodname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-1597	SourceCodester Best Church Management Software redirect.php cross site scripting	A vulnerability was found in SourceCodester Best Church Management Software 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/redirect.php. The manipulation of the argument a leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-21627	GLPI Cross-site Scripting vulnerability	GLPI is a free asset and IT management software package. In versions prior to 10.0.18, a malicious link can be crafted to perform a reflected XSS attack on the search page. If the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		anonymous ticket creation is enabled, this attack can be performed by an unauthenticated user. Version 10.0.18 contains a fix for the issue.		
CVE-2025-22513	WordPress Simple Locator Plugin <= 2.0.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Simple Locator allows Reflected XSS. This issue affects Simple Locator: from n/a through 2.0.4.	Patched by core rule	Y
CVE-2025-22564	WordPress Pretty Url Plugin <= 1.5.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Faaiq Pretty Url allows Reflected XSS. This issue affects Pretty Url: from n/a through 1.5.4.	Patched by core rule	Y
CVE-2025-22631	WordPress Marketing Automation Plugin <= 1.2.6.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vbout Marketing Automation allows Reflected XSS. This issue affects Marketing Automation: from n/a through 1.2.6.8.	Patched by core rule	Y
CVE-2025-22632	WordPress WooCommerce Pricing – Product Pricing plugin <= 1.0.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in totalsoft WooCommerce Pricing – Product Pricing allows Stored XSS. This issue affects WooCommerce Pricing – Product Pricing: from n/a through 1.0.9.	Patched by core rule	Y
CVE-2025-22635	WordPress Eventer - WordPress Event & Booking Manager Plugin plugin < 3.9.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jyothis Joy Eventer allows Reflected XSS. This issue affects Eventer: from n/a through n/a.	Patched by core rule	Y
CVE-2025-22641	WordPress FM Notification Bar plugin <= 1.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Prem Tiwari FM Notification Bar allows Stored XSS. This issue affects FM Notification Bar: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-22642	WordPress Dynamic Conditions plugin <= 1.7.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RTO GmbH Dynamic Conditions allows Stored	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		XSS. This issue affects Dynamic Conditions: from n/a through 1.7.4.		
CVE-2025-22650	WordPress Smartarget.online Integration plugin <= 1.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Erez Hadas-Sonnenschein Smartarget allows Stored XSS. This issue affects Smartarget: from n/a through 1.4.	Patched by core rule	Y
CVE-2025-22653	WordPress Music Press Pro plugin <=1.4.6 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in templaza Music Press Pro allows Stored XSS. This issue affects Music Press Pro: from n/a through 1.4.6.	Patched by core rule	Y
CVE-2025-22662	WordPress SendPulse Email Marketing Newsletter plugin <= 2.1.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SendPulse SendPulse Email Marketing Newsletter allows Stored XSS. This issue affects SendPulse Email Marketing Newsletter: from n/a through 2.1.5.	Patched by core rule	Y
CVE-2025-22664	WordPress Survey Maker Plugin <= 5.1.3.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Survey Maker team Survey Maker allows Stored XSS. This issue affects Survey Maker: from n/a through 5.1.3.5.	Patched by core rule	Y
CVE-2025-22674	WordPress Product Blocks for WooCommerce plugin <= 1.9.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Get Bowtied Product Blocks for WooCommerce allows Stored XSS. This issue affects Product Blocks for WooCommerce: from n/a through 1.9.1.	Patched by core rule	Y
CVE-2025-22675	WordPress Alert Box Block plugin <= 1.1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Alert Box Block – Display notice/alerts in the front end allows Stored XSS. This issue affects Alert Box Block – Display notice/alerts in the front end: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-22676	WordPress Upcasted S3 Offload plugin <= 3.0.3 - Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Scripting') vulnerability in upcasted AWS S3 for WordPress Plugin – Upcasted allows Stored XSS. This issue affects AWS S3 for WordPress Plugin – Upcasted: from n/a through 3.0.3.		
CVE-2025-22679	WordPress Job Board Manager Plugin <= 2.1.60 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins Job Board Manager allows Reflected XSS. This issue affects Job Board Manager: from n/a through 2.1.60.	Patched by core rule	Y
CVE-2025-22680	WordPress Ad Inserter Pro plugin <= 2.7.39 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Ad Inserter Pro allows Reflected XSS. This issue affects Ad Inserter Pro: from n/a through 2.7.39.	Patched by core rule	Y
CVE-2025-22682	WordPress Hesabfa Accounting Plugin <= 2.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hesabfa Hesabfa Accounting allows Reflected XSS. This issue affects Hesabfa Accounting: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-22683	WordPress NotificationX plugin <= 2.9.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDeveloper NotificationX allows Stored XSS. This issue affects NotificationX: from n/a through 2.9.5.	Patched by core rule	Y
CVE-2025-22684	WordPress WP BASE Booking plugin <= 5.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hakan Ozevin WP BASE Booking allows Stored XSS. This issue affects WP BASE Booking: from n/a through 5.0.0.	Patched by core rule	Y
CVE-2025-22689	WordPress Forex Calculators plugin <= 1.3.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Levan Tarbor Forex Calculators allows Stored XSS. This issue affects Forex Calculators: from n/a through 1.3.6.	Patched by core rule	Y
CVE-2025-22697	WordPress Responsive Blocks plugin <= 1.9.9 - Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Scripting') vulnerability in CyberChimps Responsive Blocks allows Reflected XSS. This issue affects Responsive Blocks: from n/a through 1.9.9.		
CVE-2025-22757	WordPress CodeBard Help Desk plugin <= 1.1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeBard CodeBard Help Desk allows Stored XSS. This issue affects CodeBard Help Desk: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-22775	WordPress Catalog Importer, Scraper & Crawler Plugin <= 5.1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in idIA Tech Catalog Importer, Scraper & Crawler allows Reflected XSS. This issue affects Catalog Importer, Scraper & Crawler: from n/a through 5.1.3.	Patched by core rule	Y
CVE-2025-22794	WordPress World Cup Predictor Plugin <= 1.9.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Landoweb Programador World Cup Predictor allows Reflected XSS. This issue affects World Cup Predictor: from n/a through 1.9.6.	Patched by core rule	Y
CVE-2025-23210	Bypass XSS sanitizer using the javascript protocol and special characters in phpoffice/phpspreadshee t	phpoffice/phpspreadsheet is a pure PHP library for reading and writing spreadsheet files. Affected versions have been found to have a Bypass of the Cross-site Scripting (XSS) sanitizer using the javascript protocol and special characters. This issue has been addressed in versions 3.9.0, 2.3.7, 2.1.8, and 1.29.9. Users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-23213	Tandoor Recipes - Stored XSS through Unrestricted File Upload	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. The file upload feature allows to upload arbitrary files, including html and svg. Both can contain malicious content (XSS Payloads). This vulnerability is fixed in 1.5.28.	Patched by core rule	Y
CVE-2025-23428	WordPress QMean plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		NotFound QMean – WordPress Did You Mean allows Reflected XSS. This issue affects QMean – WordPress Did You Mean: from n/a through 2.0.		
CVE-2025-23431	WordPress Envato Affiliater plugin <= 1.2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Envato Affiliater allows Reflected XSS. This issue affects Envato Affiliater: from n/a through 1.2.4.	Patched by core rule	Y
CVE-2025-23457	WordPress Shipdeo plugin <= 1.2.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Clodeo Shipdeo allows Reflected XSS. This issue affects Shipdeo: from n/a through 1.2.8.	Patched by core rule	Y
CVE-2025-23474	WordPress Live Dashboard plugin <= 0.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mike Martel Live Dashboard allows Reflected XSS. This issue affects Live Dashboard: from n/a through 0.3.3.	Patched by core rule	Y
CVE-2025-23491	WordPress VSTEMPLATE Creator plugin <= 2.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vikashsrivastava1111989 VSTEMPLATE Creator allows Reflected XSS. This issue affects VSTEMPLATE Creator: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-23492	WordPress 淘宝客插件 plugin <= 1.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CantonBolo WordPress 淘宝客插件 allows Reflected XSS. This issue affects WordPress 淘宝客插件: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-23523	WordPress HSS Embed Streaming Video plugin <= 3.23 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hoststreamsell HSS Embed Streaming Video allows Reflected XSS. This issue affects HSS Embed Streaming Video: from n/a through 3.23.	Patched by core rule	Y
CVE-2025-23525	WordPress Kv Compose Email From Dashboard plugin <= 1.1 - Reflected	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross Site Scripting (XSS) vulnerability	Scripting') vulnerability in kvvaradha Kv Compose Email From Dashboard allows Reflected XSS. This issue affects Kv Compose Email From Dashboard: from n/a through 1.1.		
CVE-2025-23531	WordPress RSVPMaker Volunteer Roles plugin <= 1.5.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David F. Carr RSVPMaker Volunteer Roles allows Reflected XSS. This issue affects RSVPMaker Volunteer Roles: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-23561	WordPress MLL Audio Player MP3 Ajax plugin <= 0.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound MLL Audio Player MP3 Ajax allows Stored XSS. This issue affects MLL Audio Player MP3 Ajax: from n/a through 0.7.	Patched by core rule	Y
CVE-2025-23568	WordPress WP Login Attempt Log plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fredsted WP Login Attempt Log allows Reflected XSS. This issue affects WP Login Attempt Log: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-23571	WordPress Internal Links Generator plugin <= 3.51 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Internal Links Generator allows Reflected XSS. This issue affects Internal Links Generator: from n/a through 3.51.	Patched by core rule	Y
CVE-2025-23574	WordPress CubePM plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jonathan Lau CubePM allows Reflected XSS. This issue affects CubePM: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23581	WordPress Demo User DZS plugin <= 1.1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digital Zoom Studio Demo User DZS allows Stored XSS. This issue affects Demo User DZS: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-23582	WordPress Bulk Categories Assign plugin <= 1.0 - Reflected Cross	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Site Scripting (XSS) vulnerability	Scripting') vulnerability in Haider Ali Bulk Categories Assign allows Reflected XSS. This issue affects Bulk Categories Assign: from n/a through 1.0.		
CVE-2025-23588	WordPress WOW Best CSS Compiler plugin <= 2.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WOW WordPress WOW Best CSS Compiler allows Reflected XSS. This issue affects WOW Best CSS Compiler: from n/a through 2.0.2.	Patched by core rule	Y
CVE-2025-23590	WordPress Dezdy plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Burtay Arat Dezdy allows Reflected XSS. This issue affects Dezdy: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23591	WordPress blu Logistics plugin <= 1.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Blu Logistics Pte. Ltd. blu Logistics allows Reflected XSS. This issue affects blu Logistics: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-23593	WordPress EmailPress plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound EmailPress allows Reflected XSS. This issue affects EmailPress: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23594	WordPress Google Map With Fancybox plugin <= 2.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uzzal mondal Google Map With Fancybox allows Reflected XSS. This issue affects Google Map With Fancybox: from n/a through 2.1.0.	Patched by core rule	Y
CVE-2025-23596	WordPress Notifikácie.sk plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Notifikacie.sk Notifikácie.sk allows Reflected XSS. This issue affects Notifikácie.sk: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23598	WordPress Recip.ly plugin <= 1.1.8 - Reflected Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	craig.edmunds@gmail.com Recip.ly allows Reflected XSS. This issue affects Recip.ly: from n/a through 1.1.8.		
CVE-2025-23599	WordPress eMarksheet plugin <= 5.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound eMarksheet allows Reflected XSS. This issue affects eMarksheet: from n/a through 5.0.	Patched by core rule	Y
CVE-2025-23614	WordPress WordPress Additional Logins plugin <= 1.0.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nik Sudan WordPress Additional Logins allows Reflected XSS. This issue affects WordPress Additional Logins: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-23645	WordPress Find Content IDs plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Optimize Worldwide Find Content IDs allows Reflected XSS. This issue affects Find Content IDs: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23646	WordPress Library Instruction Recorder plugin <= 1.1.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matt Brooks Library Instruction Recorder allows Reflected XSS. This issue affects Library Instruction Recorder: from n/a through 1.1.4.	Patched by core rule	Y
CVE-2025-23647	WordPress WP-Clap plugin <= 1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ariagle WP-Clap allows Reflected XSS. This issue affects WP-Clap: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-23648	WordPress AdsMiddle plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wjharil AdsMiddle allows Reflected XSS. This issue affects AdsMiddle: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23650	WordPress Tidy.ro plugin <= 1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in razvypp Tidy.ro allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Reflected XSS. This issue affects Tidy.ro: from n/a through 1.3.		
CVE-2025-23651	WordPress Scroll Top plugin <= 1.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Scroll Top allows Reflected XSS. This issue affects Scroll Top: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-23652	WordPress Add custom content after post plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Add custom content after post allows Reflected XSS. This issue affects Add custom content after post: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23653	WordPress Form To Online Booking plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Form To Online Booking allows Reflected XSS. This issue affects Form To Online Booking: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23655	WordPress Contact Form 7 – Paystack Add-on plugin <= 1.2.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Contact Form 7 – Paystack Add-on allows Reflected XSS. This issue affects Contact Form 7 – Paystack Add-on: from n/a through 1.2.3.	Patched by core rule	Y
CVE-2025-23657	WordPress WordPress-to-candidate for Salesforce CRM plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WordPress-to-candidate for Salesforce CRM allows Reflected XSS. This issue affects WordPress-to-candidate for Salesforce CRM: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23658	WordPress Advanced Angular Contact Form plugin <= 1.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tauhidul Alam Advanced Angular Contact Form allows Reflected XSS. This issue affects Advanced Angular Contact Form: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-23669	WordPress WP Smart Tooltip plugin <= 1.0.0 -	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in Nurul Amin, Mohammad Saiful Islam WP Smart Tooltip allows Stored XSS. This issue affects WP Smart Tooltip: from n/a through 1.0.0.		
CVE-2025-23671	WordPress WP OpenSearch plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fabio Savina WP OpenSearch allows Stored XSS. This issue affects WP OpenSearch: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23685	WordPress RomanCart On WordPress plugin <= 0.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound RomanCart allows Reflected XSS. This issue affects RomanCart: from n/a through 0.0.2.	Patched by core rule	Y
CVE-2025-23742	WordPress Podamibe Twilio Private Call plugin <= 1.0.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Podamibe Nepal Podamibe Twilio Private Call allows Reflected XSS. This issue affects Podamibe Twilio Private Call: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23747	WordPress Awesome Timeline plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nitesh Singh Awesome Timeline allows Stored XSS. This issue affects Awesome Timeline: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-23748	WordPress Singsys - Awesome Gallery plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Singsys -Awesome Gallery allows Reflected XSS. This issue affects Singsys - Awesome Gallery: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23750	WordPress Custom Widget Creator plugin <= 1.0.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in devbunchuk Custom Widget Creator allows Reflected XSS. This issue affects Custom Widget Creator: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-23751	WordPress Data Dash	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	plugin <= 1.2.3 - Reflected Cross Site Scripting (XSS) vulnerability	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Think201 Data Dash allows Reflected XSS. This issue affects Data Dash: from n/a through 1.2.3.	rule	
CVE-2025-23752	WordPress CGD Arrange Terms plugin <= 1.1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound CGD Arrange Terms allows Reflected XSS. This issue affects CGD Arrange Terms: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-23754	WordPress The Loops plugin <= 1.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ulrich Sossou The Loops allows Reflected XSS. This issue affects The Loops: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-23755	WordPress PAFacile plugin <= 2.6.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound PAFacile allows Reflected XSS. This issue affects PAFacile: from n/a through 2.6.1.	Patched by core rule	Y
CVE-2025-23756	WordPress LawPress plugin <= 1.4.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ivan Chernyakov LawPress – Law Firm Website Management allows Reflected XSS. This issue affects LawPress – Law Firm Website Management: from n/a through 1.4.5.	Patched by core rule	Y
CVE-2025-23759	WordPress Affiliate Tools Việt Nam plugin <= 0.3.17 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in leduchuy89vn Affiliate Tools Việt Nam allows Reflected XSS. This issue affects Affiliate Tools Việt Nam: from n/a through 0.3.17.	Patched by core rule	Y
CVE-2025-23786	WordPress Email to Download Plugin <= 3.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DuoGeek Email to Download allows Reflected XSS. This issue affects Email to Download: from n/a through 3.1.0.	Patched by core rule	Y
CVE-2025-23787	WordPress Easy Bet Plugin <= 1.0.7 -	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Reflected Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in NotFound Easy Bet allows Reflected XSS. This issue affects Easy Bet: from n/a through 1.0.7.		
CVE-2025-23788	WordPress Easy Filter Plugin <= 1.10 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Easy Filter allows Reflected XSS. This issue affects Easy Filter: from n/a through 1.10.	Patched by core rule	Y
CVE-2025-23789	WordPress URL Shortener WooCommerce Plugin <= 9.0.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tahminajannat URL Shortener | Conversion Tracking | AB Testing | WooCommerce allows Reflected XSS. This issue affects URL Shortener | Conversion Tracking | AB Testing | WooCommerce: from n/a through 9.0.2.	Patched by core rule	Y
CVE-2025-23790	WordPress Easy Code Placement Plugin <= 18.11 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wassereimer Easy Code Placement allows Reflected XSS. This issue affects Easy Code Placement: from n/a through 18.11.	Patched by core rule	Y
CVE-2025-23792	WordPress Passwordless WP – Login with your glance or fingerprint Plugin <= 1.1.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Busters Passwordless WP – Login with your glance or fingerprint allows Reflected XSS. This issue affects Passwordless WP – Login with your glance or fingerprint: from n/a through 1.1.6.	Patched by core rule	Y
CVE-2025-23799	WordPress .TUBE Video Curator Plugin <= 1.1.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in .TUBE gTLD .TUBE Video Curator allows Reflected XSS. This issue affects .TUBE Video Curator: from n/a through 1.1.9.	Patched by core rule	Y
CVE-2025-23840	WordPress WP-NOTCAPTCHA Plugin <= 1.3.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webjema WP-NOTCAPTCHA allows Reflected XSS. This issue affects WP-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		NOTCAPTCHA: from n/a through 1.3.1.		
CVE-2025-23845	WordPress ImageMeta Plugin <= 1.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ERA404 ImageMeta allows Reflected XSS. This issue affects ImageMeta: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-23851	WordPress Coronavirus (COVID-19) Outbreak Data Widgets Plugin <= 1.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Coronavirus (COVID-19) Outbreak Data Widgets allows Reflected XSS. This issue affects Coronavirus (COVID-19) Outbreak Data Widgets: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-23853	WordPress NoFollow Free plugin <= 1.6.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in michelem NoFollow Free allows Reflected XSS. This issue affects NoFollow Free: from n/a through 1.6.3.	Patched by core rule	Y
CVE-2025-23857	WordPress Essential WP Real Estate Plugin <= 1.1.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Essential WP Real Estate allows Reflected XSS. This issue affects Essential WP Real Estate: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-23905	WordPress Admin Options Pages plugin <= 0.9.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Johannes van Poelgeest Admin Options Pages allows Reflected XSS. This issue affects Admin Options Pages: from n/a through 0.9.7.	Patched by core rule	Y
CVE-2025-23920	WordPress ApplicantPro Plugin <= 1.3.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ApplicantPro ApplicantPro allows Reflected XSS. This issue affects ApplicantPro: from n/a through 1.3.9.	Patched by core rule	Y
CVE-2025-23923	WordPress Lockets Plugin <= 0.999 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Lockets allows Reflected XSS. This issue affects Lockets: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 0.999.		
CVE-2025-23975	WordPress Botnet Attack Blocker plugin <= 2.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Botnet Attack Blocker allows Stored XSS. This issue affects Botnet Attack Blocker: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-23984	WordPress Dynamic URL SEO plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainvireinfo Dynamic URL SEO allows Reflected XSS. This issue affects Dynamic URL SEO: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23987	WordPress Designer plugin <= 1.6.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodegearThemes Designer allows DOM-Based XSS. This issue affects Designer: from n/a through 1.6.0.	Patched by core rule	Y
CVE-2025-24028	Cross-site Scripting (XSS) in Rich Text Editor allows arbitrary code execution in Joplin	Joplin is a free, open source note taking and to-do application, which can handle a large number of notes organised into notebooks. This vulnerability is caused by differences between how Joplin's HTML sanitizer handles comments and how the browser handles comments. This affects both the Rich Text Editor and the Markdown viewer. However, unlike the Rich Text Editor, the Markdown viewer is `cross-origin isolated`, which prevents JavaScript from directly accessing functions/variables in the toplevel Joplin `window`. This issue is not present in Joplin 3.1.24 and may have been introduced in `9b50539`. This is an XSS vulnerability that impacts users that open untrusted notes in the Rich Text Editor. This vulnerability has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-24370	Django-Unicorn Class Pollution Vulnerability, Leading to XSS, DoS and	Django-Unicorn adds modern reactive component functionality to Django	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Authentication Bypass	templates. Affected versions of Django-Unicorn are vulnerable to python class pollution vulnerability. The vulnerability arises from the core functionality `set_property_value`, which can be remotely triggered by users by crafting appropriate component requests and feeding in values of second and third parameter to the vulnerable function, leading to arbitrary changes to the python runtime status. With this finding at least five ways of vulnerability exploitation have been observed, stably resulting in Cross-Site Scripting (XSS), Denial of Service (DoS), and Authentication Bypass attacks in almost every Django-Unicorn-based application. This issue has been addressed in version 0.62.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-24534	WordPress DPortfolio plugin <= 2.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emili Castells DPortfolio allows Reflected XSS. This issue affects DPortfolio: from n/a through 2.0.	Patched by core rule	Y
CVE-2025-24535	WordPress SKT Donation plugin <= 1.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SKT Themes SKT Donation allows Reflected XSS. This issue affects SKT Donation: from n/a through 1.9.	Patched by core rule	Y
CVE-2025-24536	WordPress ThriveDesk plugin <= 2.0.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThriveDesk ThriveDesk allows Reflected XSS. This issue affects ThriveDesk: from n/a through 2.0.6.	Patched by core rule	Y
CVE-2025-24541	WordPress DK White Label plugin <= 1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emili Castells DK White Label allows Reflected XSS. This issue affects DK White Label: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-24544	WordPress Bitcoin and Altcoin Wallets plugin <=	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	6.3.1 - Reflected Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in Alexandros Georgiou Bitcoin and Altcoin Wallets allows Reflected XSS. This issue affects Bitcoin and Altcoin Wallets: from n/a through 6.3.1.		
CVE-2025-24545	WordPress BSK Forms Validation plugin <= 1.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BannerSky.com BSK Forms Validation allows Reflected XSS. This issue affects BSK Forms Validation: from n/a through 1.7.	Patched by core rule	Y
CVE-2025-24551	WordPress Radio Buttons and Swatches for WooCommerce plugin <= 1.1.20 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OneTeamSoftware Radio Buttons and Swatches for WooCommerce allows Reflected XSS. This issue affects Radio Buttons and Swatches for WooCommerce: from n/a through 1.1.20.	Patched by core rule	Y
CVE-2025-24554	WordPress AWcode Toolkit plugin <= 1.0.14 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in awcode AWcode Toolkit allows Reflected XSS. This issue affects AWcode Toolkit: from n/a through 1.0.14.	Patched by core rule	Y
CVE-2025-24557	WordPress PlainInventory plugin <= 3.1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in plainware.com PlainInventory allows Reflected XSS. This issue affects PlainInventory: from n/a through 3.1.5.	Patched by core rule	Y
CVE-2025-24558	WordPress CRM Perks plugin <= 1.1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks CRM Perks allows Reflected XSS. This issue affects CRM Perks: from n/a through 1.1.5.	Patched by core rule	Y
CVE-2025-24559	WordPress WP Mailster plugin <= 1.8.15.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brandtoss WP Mailster allows Reflected XSS. This issue affects WP Mailster: from n/a through 1.8.15.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-24560	WordPress Awesome Event Booking plugin <= 2.7.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Awesome TOGI Awesome Event Booking allows Reflected XSS. This issue affects Awesome Event Booking: from n/a through 2.7.1.	Patched by core rule	Y
CVE-2025-24563	WordPress Cleanup – Directory Listing & Classifieds plugin <= 1.0.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGlow Cleanup – Directory Listing & Classifieds WordPress Plugin allows Reflected XSS. This issue affects Cleanup – Directory Listing & Classifieds WordPress Plugin: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-24564	WordPress Contact Form With Shortcode plugin <= 4.2.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aviplugins.com Contact Form With Shortcode allows Reflected XSS. This issue affects Contact Form With Shortcode: from n/a through 4.2.5.	Patched by core rule	Y
CVE-2025-24565	WordPress WP2LEADS plugin <= 3.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saleswonder Team Tobias WP2LEADS allows Reflected XSS. This issue affects WP2LEADS: from n/a through 3.3.3.	Patched by core rule	Y
CVE-2025-24566	WordPress Intro Tour Tutorial DeepPresentation plugin <= 6.5.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tomáš Groulík Intro Tour Tutorial DeepPresentation allows Reflected XSS. This issue affects Intro Tour Tutorial DeepPresentation: from n/a through 6.5.2.	Patched by core rule	Y
CVE-2025-24574	WordPress PeproDev WooCommerce Receipt Uploader plugin <= 2.6.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pepro Dev. Group PeproDev WooCommerce Receipt Uploader allows Reflected XSS. This issue affects PeproDev WooCommerce Receipt Uploader: from n/a through 2.6.9.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-24576	WordPress Landing Page Cat plugin <= 1.7.7 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fatcat Apps Landing Page Cat allows Reflected XSS. This issue affects Landing Page Cat: from n/a through 1.7.7.	Patched by core rule	Y
CVE-2025-24592	WordPress SysBasics Customize My Account for WooCommerce plugin <= 2.8.22 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SysBasics Customize My Account for WooCommerce allows Reflected XSS. This issue affects Customize My Account for WooCommerce: from n/a through 2.8.22.	Patched by core rule	Y
CVE-2025-24593	WordPress Edwiser Bridge plugin <= 3.0.8 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WisdmLabs Edwiser Bridge allows Reflected XSS. This issue affects Edwiser Bridge: from n/a through 3.0.8.	Patched by core rule	Y
CVE-2025-24598	WordPress WP Mailster plugin <= 1.8.17.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brandtoss WP Mailster allows Reflected XSS. This issue affects WP Mailster: from n/a through 1.8.17.0.	Patched by core rule	Y
CVE-2025-24599	WordPress Newsletters plugin <= 4.9.9.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tribulant Newsletters allows Reflected XSS. This issue affects Newsletters: from n/a through 4.9.9.6.	Patched by core rule	Y
CVE-2025-24602	WordPress WP24 Domain Check plugin <= 1.10.14 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP24 WP24 Domain Check allows Reflected XSS. This issue affects WP24 Domain Check: from n/a through 1.10.14.	Patched by core rule	Y
CVE-2025-24608	WordPress GD Mail Queue Plugin <= 4.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Milan Petrovic GD Mail Queue allows Reflected XSS. This issue affects GD Mail Queue: from n/a through 4.3.	Patched by core rule	Y
CVE-2025-24609	WordPress PORTONE	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	우커머스 결제 Plugin <= 3.2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in PortOne PORTONE 우커머스 결제 allows Reflected XSS. This issue affects PORTONE 우커머스 결제: from n/a through 3.2.4.		
CVE-2025-24614	WordPress Post Timeline Plugin <= 2.3.9 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in agileLogix Post Timeline allows Reflected XSS. This issue affects Post Timeline: from n/a through 2.3.9.	Patched by core rule	Y
CVE-2025-24615	WordPress Analytics Cat Plugin <= 1.1.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fatcatapps Analytics Cat allows Reflected XSS. This issue affects Analytics Cat: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-24616	WordPress Uix Page Builder Plugin <= 1.7.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UIUX Lab Uix Page Builder allows Reflected XSS. This issue affects Uix Page Builder: from n/a through 1.7.3.	Patched by core rule	Y
CVE-2025-24617	WordPress AcyMailing Plugin < 9.11.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AcyMailing Newsletter Team AcyMailing SMTP Newsletter allows Reflected XSS. This issue affects AcyMailing SMTP Newsletter: from n/a through n/a.	Patched by core rule	Y
CVE-2025-24620	WordPress AIO Shortcodes plugin <= 1.3 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound AIO Shortcodes allows Stored XSS. This issue affects AIO Shortcodes: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-24626	WordPress Music Store – WordPress eCommerce Plugin <= 1.1.19 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodePeople Music Store allows Reflected XSS. This issue affects Music Store: from n/a through 1.1.19.	Patched by core rule	Y
CVE-2025-24629	WordPress Import Excel to Gravity Forms Plugin <= 1.18 - Reflected Cross	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Site Scripting (XSS) vulnerability	Scripting') vulnerability in WPGear Import Excel to Gravity Forms allows Reflected XSS. This issue affects Import Excel to Gravity Forms: from n/a through 1.18.		
CVE-2025-24630	WordPress Sikshya LMS Plugin <= 0.0.21 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MantraBrain Sikshya LMS allows Reflected XSS. This issue affects Sikshya LMS: from n/a through 0.0.21.	Patched by core rule	Y
CVE-2025-24631	WordPress BP Email Assign Templates Plugin <= 1.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PhiloPress BP Email Assign Templates allows Reflected XSS. This issue affects BP Email Assign Templates: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-24632	WordPress Advanced Dynamic Pricing for WooCommerce Plugin <= 4.9.0 -Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AlgolPlus Advanced Dynamic Pricing for WooCommerce allows Reflected XSS. This issue affects Advanced Dynamic Pricing for WooCommerce: from n/a through 4.9.0.	Patched by core rule	Y
CVE-2025-24635	WordPress Paytm – Donation Plugin plugin <= 2.3.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paytm Paytm Payment Donation allows Reflected XSS. This issue affects Paytm Payment Donation: from n/a through 2.3.1.	Patched by core rule	Y
CVE-2025-24641	WordPress Better WishList API plugin <= 1.1.3 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rickonline_nl Better WishList API allows Stored XSS. This issue affects Better WishList API: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-24646	WordPress XML for Avito Plugin <= 2.5.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maxim Glazunov XML for Avito allows Reflected XSS. This issue affects XML for Avito: from n/a through 2.5.2.	Patched by core rule	Y
CVE-2025-24656	WordPress Realtyna Provisioning Plugin <=	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.2.2 - Reflected Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in Realtyna Realtyna Provisioning allows Reflected XSS. This issue affects Realtyna Provisioning: from n/a through 1.2.2.		
CVE-2025-24660	WordPress Simple Membership Custom Messages Plugin <= 2.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wp.insider Simple Membership Custom Messages allows Reflected XSS. This issue affects Simple Membership Custom Messages: from n/a through 2.4.	Patched by core rule	Y
CVE-2025-24676	WordPress Custom WP Store Locator plugin <= 1.4.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metatagg Inc Custom WP Store Locator allows Reflected XSS. This issue affects Custom WP Store Locator: from n/a through 1.4.7.	Patched by core rule	Y
CVE-2025-24680	WordPress WP Multi Store Locator Plugin <= 2.4.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in WpMultiStoreLocator WP Multi Store Locator allows Reflected XSS. This issue affects WP Multi Store Locator: from n/a through 2.4.7.	Patched by core rule	Y
CVE-2025-24684	WordPress Media Downloader Plugin <= 0.4.7.5 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ederson Peka Media Downloader allows Reflected XSS. This issue affects Media Downloader: from n/a through 0.4.7.5.	Patched by core rule	Y
CVE-2025-24686	WordPress RegistrationMagic Plugin <= 6.0.3.3 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss User Registration Forms RegistrationMagic allows Reflected XSS. This issue affects RegistrationMagic: from n/a through 6.0.3.3.	Patched by core rule	Y
CVE-2025-24688	WordPress WP Mailster Plugin <= 1.8.20.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brandtoss WP Mailster allows Reflected XSS. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects WP Mailster: from n/a through 1.8.20.0.		
CVE-2025-24700	WordPress WP Event Aggregator Plugin <= 1.8.2 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xylus Themes WP Event Aggregator allows Reflected XSS. This issue affects WP Event Aggregator: from n/a through 1.8.2.	Patched by core rule	Y
CVE-2025-24707	WordPress Photo Gallery – GT3 Image Gallery & Gutenberg Block Gallery plugin <= 2.7.7.24 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GT3 Photo Gallery Photo Gallery - GT3 Image Gallery & Gutenberg Block Gallery allows Reflected XSS. This issue affects Photo Gallery - GT3 Image Gallery & Gutenberg Block Gallery: from n/a through 2.7.7.24.	Patched by core rule	Y
CVE-2025-24708	WordPress WP Dynamics CRM plugin <= 1.1.6 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks WP Dynamics CRM for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms allows Reflected XSS. This issue affects WP Dynamics CRM for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms: from n/a through 1.1.6.	Patched by core rule	Y
CVE-2025-24710	WordPress Gwolle Guestbook plugin <= 4.7.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marcel Pol Gwolle Guestbook allows Reflected XSS. This issue affects Gwolle Guestbook: from n/a through 4.7.1.	Patched by core rule	Y
CVE-2025-24718	WordPress WP Sessions Time Monitoring Full Automatic Plugin <= 1.1.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SWIT WP Sessions Time Monitoring Full Automatic allows Reflected XSS. This issue affects WP Sessions Time Monitoring Full Automatic: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-24781	WordPress WPJobBoard plugin <= 5.10.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound WPJobBoard allows Reflected XSS. This issue affects WPJobBoard:	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		from n/a through 5.10.1.		
CVE-2025-24803	Stored Cross-Site Scripting (XSS) in MobSF	Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework. According to Apple's documentation for bundle ID's, it must contain only alphanumeric characters (A–Z, a–z, and 0–9), hyphens (-), and periods (.). However, an attacker can manually modify this value in the `Info.plist` file and add special characters to the `<key>CFBundleIdentifier</key>` value. The `dynamic_analysis.html` file does not sanitize the received bundle value from Corellium and as a result, it is possible to break the HTML context and achieve Stored XSS. This issue has been addressed in version 4.3.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-24885	pwn.college has a XSS on dojo pages	pwn.college is an education platform to learn about, and practice, core cybersecurity concepts in a hands-on fashion. Missing access control on rendering custom (unprivileged) dojo pages causes ability for users to create stored XSS.	Patched by core rule	Y
CVE-2025-24967	Stored XSS on Admin Panel When Deleting a User in reNgine	reNgine is an automated reconnaissance framework for web applications. A stored cross-site scripting (XSS) vulnerability exists in the admin panel's user management functionality. An attacker can exploit this issue by injecting malicious payloads into the username field during user creation. This vulnerability allows unauthorized script execution whenever the admin views or interacts with the affected user entry, posing a significant risk to sensitive admin functionalities. This issue affects all versions up to and including 2.20. Users are advised to monitor the project for future releases which address this issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There are no known workarounds.		
CVE-2025-24981	Parsed HTML anchor links in Markdown provided to parseMarkdown can result in XSS in @nuxtjs/mdc	MDC is a tool to take regular Markdown and write documents interacting deeply with a Vue component. In affected versions unsafe parsing logic of the URL from markdown can lead to arbitrary JavaScript code due to a bypass to the existing guards around the `javascript:` protocol scheme in the URL. The parsing logic implement in `props.ts` maintains a deny-list approach to filtering potential malicious payload. It does so by matching protocol schemes like `javascript:` and others. These security guards can be bypassed by an adversarial that provides JavaScript URLs with HTML entities encoded via hex string. Users who consume this library and perform markdown parsing from unvalidated sources could result in rendering vulnerable XSS anchor links. This vulnerability has been addressed in version 0.13.3 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-25073	WordPress Easy WP Tiles plugin <= 1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vasilis Triantafyllou Easy WP Tiles allows Stored XSS. This issue affects Easy WP Tiles: from n/a through 1.	Patched by core rule	Y
CVE-2025-25076	WordPress Graceful Email Obfuscation plugin <= 0.2.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nicholaswilson Graceful Email Obfuscation allows Stored XSS. This issue affects Graceful Email Obfuscation: from n/a through 0.2.2.	Patched by core rule	Y
CVE-2025-25077	WordPress Easy Chart Builder for WordPress plugin <= 1.3 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dugbug Easy Chart Builder for WordPress allows Stored XSS. This issue affects Easy Chart Builder for WordPress: from n/a through 1.3.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-25078	WordPress Google Earth Embed plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Andrew Norcross Google Earth Embed allows Stored XSS. This issue affects Google Earth Embed: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-25079	WordPress Simple Select All Text Box plugin <= 3.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Garrett Grimm Simple Select All Text Box allows Stored XSS. This issue affects Simple Select All Text Box: from n/a through 3.2.	Patched by core rule	Y
CVE-2025-25080	WordPress Kona Gallery Block plugin <= 1.7 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gubbigubbi Kona Gallery Block allows Stored XSS. This issue affects Kona Gallery Block: from n/a through 1.7.	Patched by core rule	Y
CVE-2025-25082	WordPress flexIDX Home Search plugin <= 2.1.2 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Max Chirkov FlexIDX Home Search allows Stored XSS. This issue affects FlexIDX Home Search: from n/a through 2.1.2.	Patched by core rule	Y
CVE-2025-25085	WordPress WP SimpleWeather plugin <= 0.2.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in matt_mcbrien WP SimpleWeather allows Stored XSS. This issue affects WP SimpleWeather: from n/a through 0.2.5.	Patched by core rule	Y
CVE-2025-25091	WordPress NextGen Cooliris Gallery plugin <= 0.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zackdesign NextGen Cooliris Gallery allows Stored XSS. This issue affects NextGen Cooliris Gallery: from n/a through 0.7.	Patched by core rule	Y
CVE-2025-25094	WordPress Breaking News Ticker plugin <= 2.4.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Amitythemes.com Breaking News Ticker allows Stored XSS. This issue affects Breaking News Ticker: from n/a through 2.4.4.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-25095	WordPress ReverbNation Widgets plugin <= 2.1 - Cross Site Scripting (XSS) vulnerability<	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in reverbnationdev ReverbNation Widgets allows Stored XSS. This issue affects ReverbNation Widgets: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-25096	WordPress RSS in Page plugin <= 2.9.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in titusbicknell RSS in Page allows Stored XSS. This issue affects RSS in Page: from n/a through 2.9.1.	Patched by core rule	Y
CVE-2025-25097	WordPress External "Video for Everybody" plugin <= 2.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kwiliarty External Video For Everybody allows Stored XSS. This issue affects External Video For Everybody: from n/a through 2.1.1.	Patched by core rule	Y
CVE-2025-25098	WordPress Links in Captions plugin <= 1.2 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zack Katz Links in Captions allows Stored XSS. This issue affects Links in Captions: from n/a through 1.2.	Patched by core rule	Y
CVE-2025-25105	WordPress Pop Up Plugin <= 0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in coffeestudios Pop Up allows Stored XSS. This issue affects Pop Up: from n/a through 0.1.	Patched by core rule	Y
CVE-2025-25117	WordPress Smart Countdown FX plugin <= 1.5.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alex Polonski Smart Countdown FX allows Stored XSS. This issue affects Smart Countdown FX: from n/a through 1.5.5.	Patched by core rule	Y
CVE-2025-25136	WordPress Optimate Ads plugin <= 1.0.3 - Cross-Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shujahat21 Optimate Ads allows Stored XSS. This issue affects Optimate Ads: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-25144	WordPress Theasys plugin <= 1.0.1 - CSRF to	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Stored XSS vulnerability	Generation ('Cross-site Scripting') vulnerability in theasys Theasys allows Stored XSS. This issue affects Theasys: from n/a through 1.0.1.		
CVE-2025-25159	WordPress WP doodlez plugin <= 1.0.10 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in robert_kolatzek WP doodlez allows Stored XSS. This issue affects WP doodlez: from n/a through 1.0.10.	Patched by core rule	Y
CVE-2025-25189	[XBOW-025-031] Reflected Cross-Site Scripting via jobid Parameter in ZOO-Project WPS publish.py CGI Script	The ZOO-Project is an open source processing platform. A reflected Cross-Site Scripting vulnerability exists in the ZOO-Project Web Processing Service (WPS) publish.py CGI script prior to commit 7a5ae1a. The script reflects user input from the `jobid` parameter in its HTTP response without proper HTML encoding or sanitization. When a victim visits a specially crafted URL pointing to this endpoint, arbitrary JavaScript code can be executed in their browser context. The vulnerability occurs because the CGI script directly outputs the query string parameters into the HTML response without escaping HTML special characters. An attacker can inject malicious JavaScript code through the `jobid` parameter which will be executed when rendered by the victim's browser. Commit 7a5ae1a contains a fix for the issue.	Patched by core rule	Y
CVE-2025-25190	[XBOW-025-033] Cross-Site Scripting (XSS) via EchoProcess Service in ZOO-Project WPS Server	The ZOO-Project is an open source processing platform. The ZOO-Project Web Processing Service (WPS) Server contains a Cross-Site Scripting (XSS) vulnerability in its EchoProcess service prior to commit 7a5ae1a. The vulnerability exists because the EchoProcess service directly reflects user input in its output without proper sanitization when handling complex inputs.The service accepts various input formats including XML, JSON, and SVG, and returns the content based on the requested MIME type. When processing SVG content and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		returning it with the image/svg+xml MIME type, the server fails to sanitize potentially malicious JavaScript in attributes like onload, allowing arbitrary JavaScript execution in the victim's browser context. This vulnerability is particularly dangerous because it exists in a service specifically designed to echo back user input, and the lack of proper sanitization in combination with SVG handling creates a reliable XSS vector. Commit 7a5ae1a contains a fix for the issue.		
CVE-2025-25203	Ctrlpanel has stored XSS vulnerability in TicketsController priority field	CtrlPanel is open-source billing software for hosting providers. Prior to version 1.0, a Cross-Site Scripting (XSS) vulnerability exists in the `TicketsController` and `Moderation/TicketsController` due to insufficient input validation on the `priority` field during ticket creation and unsafe rendering of this field in the moderator panel. Version 1.0 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-25287	Lakeus vulnerable to stored XSS via system messages	Lakeus is a simple skin made for MediaWiki. Starting in version 1.8.0 and prior to versions 1.3.1+REL1.39, 1.3.1+REL1.42, and 1.4.0, Lakeus is vulnerable to store cross-site scripting via malicious system messages, though editing the messages requires high privileges. Those with `(editinterface)` rights can edit system messages that are improperly handled in order to send raw HTML. In the case of `lakeus-footermessage`, this will affect all users if the server is configured to link back to this repository. Otherwise, the system messages in themeDesigner.js are only used when the user enables it in their preferences. Versions 1.3.1+REL1.39, 1.3.1+REL1.42, and 1.4.0 contain a patch.	Patched by core rule	Y
CVE-2025-25296	Label Studio allows Cross-Site Scripting (XSS) via GET request to `/projects/upload-example` endpoint	Label Studio is an open source data labeling tool. Prior to version 1.16.0, Label Studio's `/projects/upload-example` endpoint allows injection of arbitrary HTML	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through a `GET` request with an appropriately crafted `label_config` query parameter. By crafting a specially formatted XML label config with inline task data containing malicious HTML/JavaScript, an attacker can achieve Cross-Site Scripting (XSS). While the application has a Content Security Policy (CSP), it is only set in report-only mode, making it ineffective at preventing script execution. The vulnerability exists because the upload-example endpoint renders user-provided HTML content without proper sanitization on a GET request. This allows attackers to inject and execute arbitrary JavaScript in victims' browsers by getting them to visit a maliciously crafted URL. This is considered vulnerable because it enables attackers to execute JavaScript in victims' contexts, potentially allowing theft of sensitive data, session hijacking, or other malicious actions. Version 1.16.0 contains a patch for the issue.		
CVE-2025-25299	Cross-site scripting (XSS) in the real-time collaboration package	CKEditor 5 is a modern JavaScript rich-text editor with an MVC architecture. During a recent internal audit, a Cross-Site Scripting (XSS) vulnerability was discovered in the CKEditor 5 real-time collaboration package. This vulnerability affects user markers, which represent users' positions within the document. It can lead to unauthorized JavaScript code execution, which might happen with a very specific editor and token endpoint configuration. This vulnerability affects only installations with Real-time collaborative editing enabled. The problem has been recognized and patched. The fix is available in version 44.2.1 (and above). Users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-25304	Vega allows Cross-site Scripting via the vlSelectionTuples function	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. Prior to version 5.26.0 of vega and 5.4.2 of vega-selections, the `vlSelectionTuples` function can be used to call JavaScript functions, leading to cross-site scripting.`vlSelectionTuples` calls multiple functions that can be controlled by an attacker, including one call with an attacker-controlled argument. This can be used to call `Function()` with arbitrary JavaScript and the resulting function can be called with `vlSelectionTuples` or using a type coercion to call `toString` or `valueOf`. Version 5.26.0 of vega and 5.4.2 of vega-selections fix this issue.	Patched by core rule	Y
CVE-2025-26538	WordPress Prezi Embedder plugin <= 2.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dan Rossiter Prezi Embedder allows Stored XSS. This issue affects Prezi Embedder: from n/a through 2.1.	Patched by core rule	Y
CVE-2025-26539	WordPress Embed Google Map plugin <= 3.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in petkivim Embed Google Map allows Stored XSS. This issue affects Embed Google Map: from n/a through 3.2.	Patched by core rule	Y
CVE-2025-26551	WordPress Bootstrap collapse plugin <= 1.0.4 - CSRF to Stored Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sureshdsk Bootstrap collapse allows Stored XSS. This issue affects Bootstrap collapse: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-26552	WordPress Naver Syndication V2 plugin <= 0.8.3 - CSRF to Stored Cross-Site Scripting vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in badrHan Naver Syndication V2 allows Stored XSS. This issue affects Naver Syndication V2: from n/a through 0.8.3.	Patched by core rule	Y
CVE-2025-26558	WordPress Aparat Responsive plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		mkkmail Aparat Responsive allows DOM-Based XSS. This issue affects Aparat Responsive: from n/a through 1.3.		
CVE-2025-26561	WordPress Elfsight Yottie Lite Plugin <= 1.3.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in elfsight Elfsight Yottie Lite allows Stored XSS. This issue affects Elfsight Yottie Lite: from n/a through 1.3.3.	Patched by core rule	Y
CVE-2025-26567	WordPress Font Awesome WP plugin <= 1.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in farjana55 Font Awesome WP allows DOM-Based XSS. This issue affects Font Awesome WP: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-26574	WordPress Google Drive WP Media plugin <= 2.4.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Moch Amir Google Drive WP Media allows Stored XSS. This issue affects Google Drive WP Media: from n/a through 2.4.4.	Patched by core rule	Y
CVE-2025-26751	WordPress Alphabetic Pagination Plugin <= 3.2.1 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fahad Mahmood Alphabetic Pagination allows Reflected XSS. This issue affects Alphabetic Pagination: from n/a through 3.2.1.	Patched by core rule	Y
CVE-2025-26754	WordPress Timeline Block plugin <= 1.1.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Timeline Block allows Stored XSS. This issue affects Timeline Block: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-26756	WordPress Magic the Gathering Card Tooltips plugin <= 3.5.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in grimdonkey Magic the Gathering Card Tooltips allows Stored XSS. This issue affects Magic the Gathering Card Tooltips: from n/a through 3.5.0.	Patched by core rule	Y
CVE-2025-26761	WordPress Easy Elementor Addons plugin <= 2.1.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HashThemes Easy Elementor Addons allows DOM-Based	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		XSS. This issue affects Easy Elementor Addons: from n/a through 2.1.5.		
CVE-2025-26766	WordPress Leyka plugin <= 3.31.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VaultDweller Leyka allows Stored XSS. This issue affects Leyka: from n/a through 3.31.8.	Patched by core rule	Y
CVE-2025-26767	WordPress Qubely – Advanced Gutenberg Blocks plugin <= 1.8.12 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Qubely – Advanced Gutenberg Blocks allows Stored XSS. This issue affects Qubely – Advanced Gutenberg Blocks: from n/a through 1.8.12.	Patched by core rule	Y
CVE-2025-26769	WordPress Vertex Addons for Elementor plugin <= 1.2.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webilia Inc. Vertex Addons for Elementor allows Stored XSS. This issue affects Vertex Addons for Elementor: from n/a through 1.2.0.	Patched by core rule	Y
CVE-2025-26770	WordPress Waymark plugin <= 1.5.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joe Waymark allows Stored XSS. This issue affects Waymark: from n/a through 1.5.0.	Patched by core rule	Y
CVE-2025-26771	WordPress SKT Blocks plugin <= 1.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sonalsinha21 SKT Blocks – Gutenberg based Page Builder allows Stored XSS. This issue affects SKT Blocks – Gutenberg based Page Builder: from n/a through 1.7.	Patched by core rule	Y
CVE-2025-26772	WordPress DethemeKit For Elementor plugin <= 2.1.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Detheme DethemeKit For Elementor allows Stored XSS. This issue affects DethemeKit For Elementor: from n/a through 2.1.8.	Patched by core rule	Y
CVE-2025-26774	WordPress Responsive Modal Builder for High Conversion – Easy Popups plugin <= 1.5.0 - Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rock Solid Responsive Modal	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Builder for High Conversion – Easy Popups allows Reflected XSS. This issue affects Responsive Modal Builder for High Conversion – Easy Popups: from n/a through 1.5.0.		
CVE-2025-26775	WordPress BEAR Plugin <= 1.1.4.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 BEAR allows Stored XSS. This issue affects BEAR: from n/a through 1.1.4.4.	Patched by core rule	Y
CVE-2025-26778	WordPress Gallery Custom Links Plugin <= 2.2.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Gallery allows Stored XSS. This issue affects Gallery: from n/a through 2.2.1.	Patched by core rule	Y
CVE-2025-26791	N/A	DOMPurify before 3.2.4 has an incorrect template literal regular expression, sometimes leading to mutation cross-site scripting (mXSS).	Patched by core rule	Y
CVE-2025-26868	WordPress Fast Flow plugin <= 1.2.16 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in fastflow Fast Flow allows Reflected XSS. This issue affects Fast Flow: from n/a through 1.2.16.	Patched by core rule	Y
CVE-2025-26877	WordPress Front End Users Plugin <= 3.2.30 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rustaurius Front End Users allows Stored XSS. This issue affects Front End Users: from n/a through 3.2.30.	Patched by core rule	Y
CVE-2025-26878	WordPress Autoship Cloud for WooCommerce Subscription Products plugin <= 2.8.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in patternsinthecloud Autoship Cloud for WooCommerce Subscription Products allows DOM-Based XSS. This issue affects Autoship Cloud for WooCommerce Subscription Products: from n/a through 2.8.0.1.	Patched by core rule	Y
CVE-2025-26881	WordPress Sticky Content plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Sticky Content allows Stored XSS. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects Sticky Content: from n/a through 1.0.1.		
CVE-2025-26882	WordPress Popup Builder plugin <= 1.1.33 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Popup Builder allows Stored XSS. This issue affects Popup Builder: from n/a through 1.1.33.	Patched by core rule	Y
CVE-2025-26884	WordPress Greenshift plugin <= 10.8 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpsoul Greenshift allows Stored XSS. This issue affects Greenshift: from n/a through 10.8.	Patched by core rule	Y
CVE-2025-26887	WordPress EZ SQL Reports Shortcode Widget and DB Backup plugin <= 5.21.35 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Eli EZ SQL Reports Shortcode Widget and DB Backup allows Stored XSS. This issue affects EZ SQL Reports Shortcode Widget and DB Backup: from n/a through 5.21.35.	Patched by core rule	Y
CVE-2025-26891	WordPress Ibtana – WordPress Website Builder plugin <= 1.2.4.9 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VW THEMES Ibtana allows Stored XSS. This issue affects Ibtana: from n/a through 1.2.4.9.	Patched by core rule	Y
CVE-2025-26893	WordPress Easy Charts plugin <= 1.2.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kiran Potphode Easy Charts allows DOM-Based XSS. This issue affects Easy Charts: from n/a through 1.2.3.	Patched by core rule	Y
CVE-2025-26896	WordPress PiwigoPress plugin <= 2.33 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vpiwigo PiwigoPress allows Stored XSS. This issue affects PiwigoPress: from n/a through 2.33.	Patched by core rule	Y
CVE-2025-26897	WordPress List Related Attachments plugin <= 2.1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Baden List Related Attachments allows DOM-Based XSS. This issue affects List Related Attachments: from n/a through 2.1.6.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-26904	WordPress WP Responsive Auto Fit Text plugin <= 0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gal_op WP Responsive Auto Fit Text allows DOM-Based XSS. This issue affects WP Responsive Auto Fit Text: from n/a through 0.2.	Patched by core rule	Y
CVE-2025-26907	WordPress Estatik Mortgage Calculator plugin <= 2.0.12 - Local File Inclusion vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Estatik Mortgage Calculator Estatik allows Stored XSS. This issue affects Mortgage Calculator Estatik: from n/a through 2.0.12.	Patched by core rule	Y
CVE-2025-26912	WordPress Easy Elementor Addons plugin <= 2.1.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HashThemes Easy Elementor Addons allows Stored XSS. This issue affects Easy Elementor Addons: from n/a through 2.1.6.	Patched by core rule	Y
CVE-2025-26913	WordPress AR for WordPress plugin <= 7.7 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webandprint AR For WordPress allows DOM-Based XSS. This issue affects AR For WordPress: from n/a through 7.7.	Patched by core rule	Y
CVE-2025-26937	WordPress Icon List Block plugin <= 1.1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Icon List Block allows Stored XSS. This issue affects Icon List Block: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-26938	WordPress Countdown Timer block plugin <= 1.2.6 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Countdown Timer allows Stored XSS. This issue affects Countdown Timer: from n/a through 1.2.6.	Patched by core rule	Y
CVE-2025-26939	WordPress Counters Block plugin <= 1.1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Counters Block allows Stored XSS. This issue affects Counters Block: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-26945	WordPress Info Cards plugin <= 1.0.5 - Cross Site Scripting (XSS)	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability	Scripting') vulnerability in bPlugins Info Cards – Gutenberg block for creating Beautiful Cards allows Stored XSS. This issue affects Info Cards – Gutenberg block for creating Beautiful Cards: from n/a through 1.0.5.		
CVE-2025-26947	WordPress Services Section block plugin <= 1.3.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Services Section block allows Stored XSS. This issue affects Services Section block: from n/a through 1.3.4.	Patched by core rule	Y
CVE-2025-26949	WordPress Team Section Block plugin <= 1.0.9 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Team Section Block allows Stored XSS. This issue affects Team Section Block: from n/a through 1.0.9.	Patched by core rule	Y
CVE-2025-26952	WordPress Business Card Block plugin <= 1.0.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins Business Card Block allows Stored XSS. This issue affects Business Card Block: from n/a through 1.0.5.	Patched by core rule	Y
CVE-2025-26962	WordPress Contact Form Plugin plugin <= 1.1.25 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GhozyLab Easy Contact Form Lite allows Stored XSS. This issue affects Easy Contact Form Lite : from n/a through 1.1.25.	Patched by core rule	Y
CVE-2025-26973	WordPress Social Warfare Plugin <= 4.5.4 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WarfarePlugins Social Warfare allows DOM-Based XSS. This issue affects Social Warfare: from n/a through 4.5.4.	Patched by core rule	Y
CVE-2025-26980	WordPress Wired Impact Volunteer Management plugin <= 2.5 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wired Impact Wired Impact Volunteer Management allows Stored XSS. This issue affects Wired Impact Volunteer Management: from n/a through 2.5.	Patched by core rule	Y
CVE-2025-26981	WordPress Web Accessibility By accessiBe	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	plugin <= 2.5 - Reflected Cross Site Scripting (XSS) vulnerability	Generation ('Cross-site Scripting') vulnerability in accessiBe Web Accessibility By accessiBe allows Reflected XSS. This issue affects Web Accessibility By accessiBe: from n/a through 2.5.		
CVE-2025-26987	WordPress Frontend Admin by DynamiApps plugin <= 3.25.17 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shabti Kaplan Frontend Admin by DynamiApps allows Reflected XSS. This issue affects Frontend Admin by DynamiApps: from n/a through 3.25.17.	Patched by core rule	Y
CVE-2025-26991	WordPress WPPizza plugin <= 3.19.4 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ollybach WPPizza allows Reflected XSS. This issue affects WPPizza: from n/a through 3.19.4.	Patched by core rule	Y
CVE-2025-26993	WordPress Visual Website Collaboration Atarim plugin <= 4.1.0 - Reflected Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vito Peleg Atarim allows Reflected XSS. This issue affects Atarim: from n/a through 4.1.0.	Patched by core rule	Y
CVE-2025-27016	WordPress Drivr Lite – Google Drive Plugin plugin <= 1.0.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in awsm.in Drivr Lite – Google Drive Plugin allows Stored XSS. This issue affects Drivr Lite – Google Drive Plugin: from n/a through 1.0.1.	Patched by core rule	Y
CVE-2025-27088	Reflected Cross-site Scripting (XSS) in template implementation in oxyno-zeta/s3-proxy	oxyno-zeta/s3-proxy is an aws s3 proxy written in go. In affected versions a Reflected Cross-site Scripting (XSS) vulnerability enables attackers to create malicious URLs that, when visited, inject scripts into the web application. This can lead to session hijacking or phishing attacks on a trusted domain, posing a moderate risk to all users. It's possible to inject html elements, including scripts through the folder-list template. The affected template allows users to interact with the URL path provided by the `Request.URL.Path` variable, which is then rendered	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		directly into the HTML without proper sanitization or escaping. This can be abused by attackers who craft a malicious URL containing injected HTML or JavaScript. When users visit such a URL, the malicious script will be executed in the user's context. This issue has been addressed in version 4.18.1 and all users are advised to upgrade. There are no known workarounds for this vulnerability.		
CVE-2025-27108	Cross-site Scripting vulnerability due to improper use of string.replace in dom-expressions	dom-expressions is a Fine-Grained Runtime for Performant DOM Rendering. In affected versions the use of javascript's `.replace()` opens up to potential Cross-site Scripting (XSS) vulnerabilities with the special replacement patterns beginning with `$`. Particularly, when the attributes of `Meta` tag from solid-meta are user-defined, attackers can utilise the special replacement patterns, either `$'` or `$\`` to achieve XSS. The solid-meta package has this issue since it uses `useAffect` and context providers, which injects the used assets in the html header. "dom-expressions" uses `.replace()` to insert the assets, which is vulnerable to the special replacement patterns listed above. This effectively means that if the attributes of an asset tag contained user-controlled data, it would be vulnerable to XSS. For instance, there might be meta tags for the open graph protocol in a user profile page, but if attackers set the user query to some payload abusing `.replace()`, then they could execute arbitrary javascript in the victim's web browser. Moreover, it could be stored and cause more problems. This issue has been addressed in version 0.39.5 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	Patched by core rule	Y
CVE-2025-27139	Combodo iTop vulnerable to stored self Cross-site Scripting in preferences	Combodo iTop is a web based IT service management tool. Versions	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		prior to 2.7.12, 3.1.2, and 3.2.0 are vulnerable to cross-site scripting when the preferences page is opened. Versions 2.7.12, 3.1.2, and 3.2.0 fix the issue.		
CVE-2025-27145	copyparty renders unsanitized filenames as HTML when user uploads empty files	copyparty, a portable file server, has a DOM-based cross-site scripting vulnerability in versions prior to 1.16.15. The vulnerability is considered low-risk. By handing someone a maliciously-named file, and then tricking them into dragging the file into copyparty's Web-UI, an attacker could execute arbitrary javascript with the same privileges as that user. For example, this could give unintended read-access to files owned by that user. The bug is triggered by the drag-drop action itself; it is not necessary to actually initiate the upload. The file must be empty (zero bytes). Note that, as a general-purpose webserver, it is intentionally possible to upload HTML-files with arbitrary javascript in `<script>` tags, which will execute when the file is opened. The difference is that this vulnerability would trigger execution of javascript during the act of uploading, and not when the uploaded file was opened. Version 1.16.15 contains a fix.	Patched by core rule	Y
CVE-2025-27265	WordPress Google Maps for WordPress plugin <= 1.0.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aaron D. Campbell Google Maps for WordPress allows DOM-Based XSS. This issue affects Google Maps for WordPress: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-27266	WordPress Hover Image Button plugin <= 1.1.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ignacio Perez Hover Image Button allows DOM-Based XSS. This issue affects Hover Image Button: from n/a through 1.1.2.	Patched by core rule	Y
CVE-2025-27280	WordPress Archive Page plugin <= 1.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Alobaidi Archive Page allows DOM-Based XSS. This issue affects Archive Page: from n/a through 1.0.1.		
CVE-2025-27303	WordPress Contact Form 7 Star Rating plugin <= 1.10 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themelogger Contact Form 7 Star Rating allows Stored XSS. This issue affects Contact Form 7 Star Rating: from n/a through 1.10.	Patched by core rule	Y
CVE-2025-27304	WordPress Contact Form 7 Star Rating with font Awesome plugin <= 1.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themelogger Contact Form 7 Star Rating with font Awesome allows Stored XSS. This issue affects Contact Form 7 Star Rating with font Awesome: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-27305	WordPress Table of Contents Block plugin <= 1.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Achal Jain Table of Contents Block allows Stored XSS. This issue affects Table of Contents Block: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-27306	WordPress Pathomation plugin <= 2.5.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pathomation Pathomation allows Stored XSS. This issue affects Pathomation: from n/a through 2.5.1.	Patched by core rule	Y
CVE-2025-27307	WordPress Quotes llama plugin <= 3.0.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in oooorgle Quotes llama allows Reflected XSS. This issue affects Quotes llama: from n/a through 3.0.1.	Patched by core rule	Y
CVE-2025-27320	WordPress Profile Widget Ninja plugin <= 4.3 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pankaj Mondal Profile Widget Ninja allows DOM-Based XSS. This issue affects Profile Widget Ninja: from n/a through 4.3.	Patched by core rule	Y
CVE-2025-27323	WordPress WP About Author plugin <= 1.5 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jon Bishop WP About Author	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows DOM-Based XSS. This issue affects WP About Author: from n/a through 1.5.		
CVE-2025-27325	WordPress Video.js HLS Player plugin <= 1.0.2 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bruce Video.js HLS Player allows DOM-Based XSS. This issue affects Video.js HLS Player: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-27327	WordPress Live Streaming Video Player – by SRS Player plugin <= 1.0.18 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Winlin Live Streaming Video Player – by SRS Player allows DOM-Based XSS. This issue affects Live Streaming Video Player – by SRS Player: from n/a through 1.0.18.	Patched by core rule	Y
CVE-2025-27329	WordPress EZ InLinkz linkup plugin <= 0.18 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in inlinkz EZ InLinkz linkup allows DOM-Based XSS. This issue affects EZ InLinkz linkup: from n/a through 0.18.	Patched by core rule	Y
CVE-2025-27330	WordPress PlayerJS plugin <= 2.23 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PlayerJS PlayerJS allows DOM-Based XSS. This issue affects PlayerJS: from n/a through 2.23.	Patched by core rule	Y
CVE-2025-27331	WordPress WooCommerce Display Products by Tags plugin <= 1.0.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sébastien Dumont WooCommerce Display Products by Tags allows DOM-Based XSS. This issue affects WooCommerce Display Products by Tags: from n/a through 1.0.0.	Patched by core rule	Y
CVE-2025-27341	WordPress Reactive Mortgage Calculator plugin <= 1.1 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in afzal_du Reactive Mortgage Calculator allows Stored XSS. This issue affects Reactive Mortgage Calculator: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-27347	WordPress Direct Checkout Button for WooCommerce plugin <=	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.0 - Cross Site Scripting (XSS) vulnerability	Scripting') vulnerability in techmix Direct Checkout Button for WooCommerce allows Stored XSS. This issue affects Direct Checkout Button for WooCommerce: from n/a through 1.0.		
CVE-2025-27348	WordPress WP Social SEO Booster plugin <= 1.2.0 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Daniel WP Social SEO Booster – Knowledge Graph Social Signals SEO allows Stored XSS. This issue affects WP Social SEO Booster – Knowledge Graph Social Signals SEO: from n/a through 1.2.0.	Patched by core rule	Y
CVE-2025-27349	WordPress Get Posts plugin <= 0.6 - Stored Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nurelm Get Posts allows Stored XSS. This issue affects Get Posts: from n/a through 0.6.	Patched by core rule	Y
CVE-2025-27351	WordPress Local Search SEO Contact Page plugin <= 4.0.1 - Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ExpertBusinessSearch Local Search SEO Contact Page allows Stored XSS. This issue affects Local Search SEO Contact Page: from n/a through 4.0.1.	Patched by core rule	Y
CVE-2025-27352	WordPress plugin <= 1.0.5.7 - CSRF to Cross Site Scripting (XSS) vulnerability	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wumii team allows Stored XSS. This issue affects: from n/a through 1.0.5.7.	Patched by core rule	Y

INDUSFACE™

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine.

Indusface, an institutionally funded firm, is the only vendor to receive 100% customer recommendation rating four years in a row and is a global customer choice in the 2024 Gartner Peer Insights™ Web Application and API Protection (WAAP) Report. Indusface is also a “Great Place to Work” 2024 certified and is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards.

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™