INDUSFACE™

# Monthly Zero-Day Vulnerability Coverage Report

August 2025

## The total zero-day vulnerabilities count for August month: 459

| Command Injection | SQL Injection | SSRF | Path Traversal | Cross-Site Scripting |
|---|---|---|---|---|
| 35 | 67 | 16 | 68 | 273 |

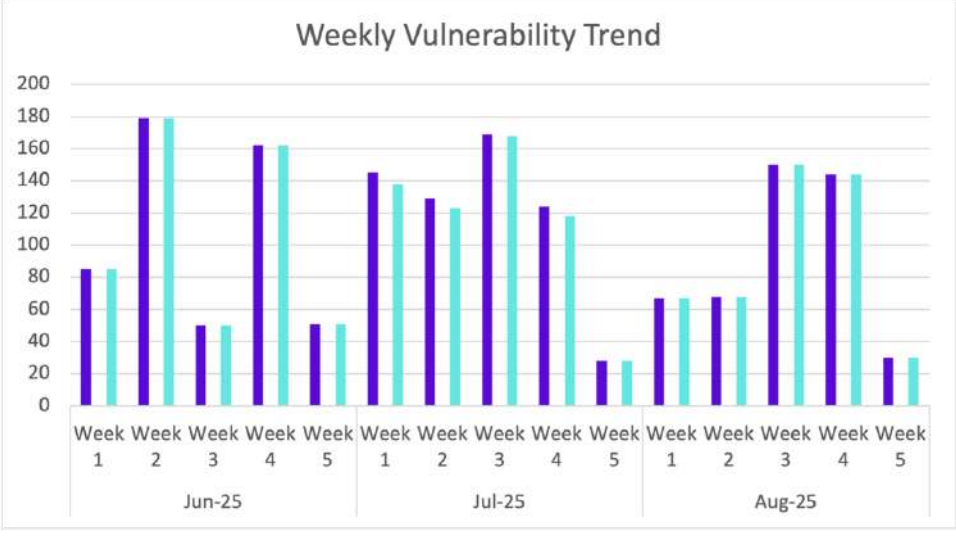
| | |
|---|---|
| Zero-day vulnerabilities protected through core rules | 459 |
| Zero-day vulnerabilities protected through custom rules | 0 |
| Zero-day vulnerabilities found by Indusface WAS | 459 |

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

## Vulnerability Trend:

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

## Weekly Vulnerability Trend

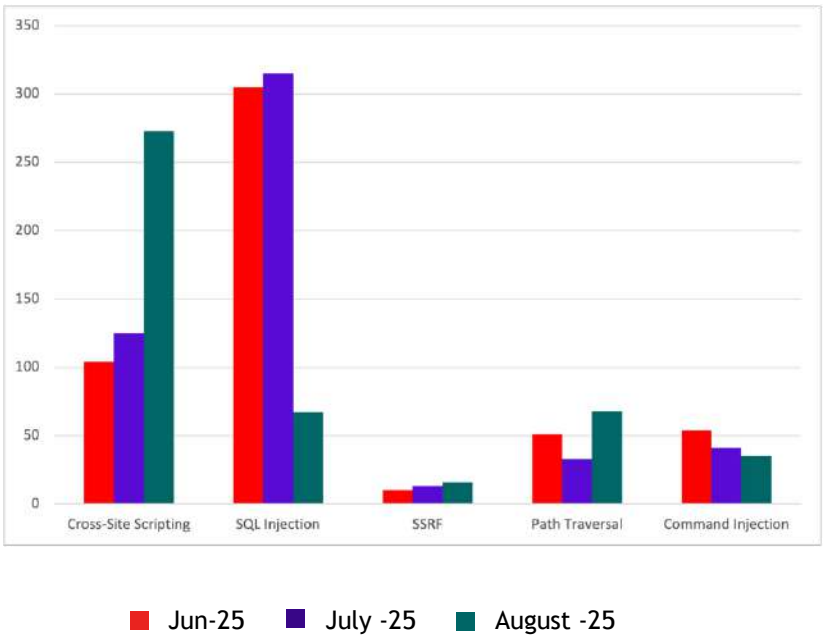




of the zero-day vulnerabilities were protected by the core rules in the last month


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

Top Five Vulnerability Categories




# Vulnerability Details

## Command Injection Vulnerabilities

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-50722 | CVE-2025 - Insecure Permissions vulnerability in sparkshop v.1.1.7 allows a remote attacker to execute arbitrar... | Insecure Permissions vulnerability in sparkshop v.1.1.7 allows a remote attacker to execute arbitrary code via the Common.php component | Patched by core rule | Y |
| CVE-2025-29523 | CVE-2025 - D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command inject... | D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command injection vulnerability via the ping6 function. | Patched by core rule | Y |
| CVE-2025-44179 | CVE-2025 - Hitron CGNF-TWN 3.1.1.43-TWN-pre3 contains a command injection vulnerability in the telnet service. ... | Hitron CGNF-TWN 3.1.1.43-TWN-pre3 contains a command injection vulnerability in the telnet service. The issue arises due to improper input validation within the telnet command handling mechanism. An attacker can exploit this vulnerability by injecting arbitrary commands through the telnet interface when prompted for inputs or commands. Successful exploitation could lead to remote code execution (RCE) under the privileges of the telnet user, potentially allowing unauthorized access to system settings and sensitive information. | Patched by core rule | Y |
| CVE-2025-29522 | CVE-2025 - D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command inject... | D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command injection vulnerability via the ping function. | Patched by core rule | Y |
| CVE-2025-29519 | CVE-2025 - A command injection vulnerability in the EXE parameter of D-Link DSL-7740C with | A command injection vulnerability in the EXE parameter of D-Link DSL-7740C with firmware | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | firmware DSL7740C.V6... | DSL7740C.V6.TR069.20211230 allows attackers to execute arbitrary commands via supplying a crafted GET request. | | |
| CVE-2025-29517 | CVE-2025 - D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command inject... | D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command injection vulnerability via the traceroute6 function. | Patched by core rule | Y |
| CVE-2025-29516 | CVE-2025 - D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command inject... | D-Link DSL-7740C with firmware DSL7740C.V6.TR069.20211230 was discovered to contain a command injection vulnerability via the backup function. | Patched by core rule | Y |
| CVE-2025-9387 | CVE-2025 - A vulnerability was found in DCN DCME-720 9.1.5.11. This affects an unknown function of the file /us... | A vulnerability was found in DCN DCME-720 9.1.5.11. This affects an unknown function of the file /usr/local/www/function/audit/newstatistics/ip_block.php of the component Web Management Backend. Performing manipulation of the argument ip results in os command injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. Other products might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-43762 | CVE-2025 - Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.1, 2024.Q4.0 throu... | Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.1, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allow users to upload an unlimited amount of files through the forms, the files are stored in the document_library allowing an attacker to cause a potential DDoS. | Patched by core rule | Y |
| CVE-2025-43752 | CVE-2025 - Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4, 2024.Q4.0 throu... | Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15 and 7.4 GA through update 92 allow users to upload an unlimited amount of files through the object entries attachment fields, the files are stored in the document_library allowing an attacker to cause a potential DDoS. | Patched by core rule | Y |
| CVE-2025-9262 | CVE-2025 - A flaw has been found in wong2 mcp-cli 1.13.0. Affected is the function redirectToAuthorization of t... | A flaw has been found in wong2 mcp-cli 1.13.0. Affected is the function redirectToAuthorization of the file /src/oauth/provider.js of the component oAuth Handler. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | This manipulation causes os command injection. The attack may be initiated remotely. The attack is considered to have high complexity. The exploitability is told to be difficult. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | | |
| CVE-2025-9244 | CVE-2025 - A security vulnerability has been detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9... | A security vulnerability has been detected in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 1.0.013.001/1.0.04.001/1.0.04.002/1.1.05.003/1.2.07.001. This vulnerability affects the function addStaticRoute of the file /goform/addStaticRoute. Such manipulation of the argument staticRoute_IP_setting/staticRoute_Netmask_setting/staticRoute_Gateway_setting/staticRoute_Metric_setting/staticRoute_destType_setting leads to os command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-52337 | CVE-2025 - An authenticated arbitrary file upload vulnerability in the Content Explorer feature of LogicData eC... | An authenticated arbitrary file upload vulnerability in the Content Explorer feature of LogicData eCommerce Framework v5.0.9.7000 allows attackers to execute arbitrary code via uploading a crafted file. | Patched by core rule | Y |
| CVE-2025-50461 | CVE-2025 - A deserialization vulnerability exists in Volcengine's verl 3.0.0, specifically in the scripts/model... | A deserialization vulnerability exists in Volcengine's verl 3.0.0, specifically in the scripts/model_merger.py script when using the "fsdp" backend. The script calls torch.load() with weights_only=False on user-supplied .pt files, allowing attackers to execute arbitrary code if a maliciously crafted model file is loaded. An attacker can exploit this by convincing a victim to download and place a malicious model file in a local directory with a specific filename pattern. This vulnerability may lead to arbitrary code execution with the privileges of the user running the script. | Patched by core rule | Y |
| CVE-2025-55591 | CVE-2025 - TOTOLINK-A3002R v4.0.0-B20230531.1404 was discovered to contain a command injection vulnerability in... | TOTOLINK-A3002R v4.0.0-B20230531.1404 was discovered to contain a command injection vulnerability in the devicemac parameter in the formMapDel endpoint. | Patched by core rule | Y |
| CVE-2025-55590 | CVE-2025 - TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain an | TOTOLINK A3002R v4.0.0-B20230531.1404 was discovered to contain an command injection | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | command injection vulnerability v... | vulnerability via the component bupload.html. | | |
| CVE-2025-50515 | CVE-2025 - An issue was discovered in phome Empirebak 2010 in ebak2008/upload/class/config.php allowing attacke... | An issue was discovered in phome Empirebak 2010 in ebak2008/upload/class/config.php allowing attackers to execute arbitrary code when the config file was loaded. | Patched by core rule | Y |
| CVE-2024-53945 | CVE-2025 - The KuWFi 4G AC900 LTE router 1.0.13 is vulnerable to command injection on the HTTP API endpoints /g... | The KuWFi 4G AC900 LTE router 1.0.13 is vulnerable to command injection on the HTTP API endpoints /goform/formMultiApnSetting and /goform/atCmd. An authenticated attacker can execute arbitrary OS commands with root privileges via shell metacharacters in parameters such as pincode and cmds. Exploitation can lead to full system compromise, including enabling remote access (e.g., enabling telnet). | Patched by core rule | Y |
| CVE-2025-45317 | CVE-2025 - A zip slip vulnerability in the /modules/ImportModule.php component of hortusfox-web v4.4 allows att... | A zip slip vulnerability in the /modules/ImportModule.php component of hortusfox-web v4.4 allows attackers to execute arbitrary code via a crafted archive. | Patched by core rule | Y |
| CVE-2025-43736 | CVE-2025 - A Denial Of Service via File Upload (DOS) vulnerability in the Liferay Portal 7.4.3.0 through 7.4.3.... | A Denial Of Service via File Upload (DOS) vulnerability in the Liferay Portal 7.4.3.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.8, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 GA through update 92 allows a user to upload more than 300kb profile picture into the user profile. This size more than the noted max 300kb size. This extra amount of data can make Liferay slower. | Patched by core rule | Y |
| CVE-2025-8830 | CVE-2025 - A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20... | A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this issue is the function sub_3517C of the file /goform/setWan. The manipulation of the argument Hostname leads to os command 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-2025-8829 | CVE-2025 - A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20... | A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this vulnerability is the function um_red of the file /goform/RP_setBasicAuto. The manipulation of the argument hname leads to os command injection. The attack can be launched | 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. The vendor was contacted early about this disclosure but did not respond in any way. | | |
| CVE-2025-8828 | CVE-2025 - A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20... | A vulnerability was determined in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected is the function ipv6cmd of the file /goform/setIpv6. The manipulation of the argument Ipv6PriDns/Ipv6SecDns/Ipv6StaticGateway/LanIpv6Addr/LanPrefixLen/pppoeUser/pppoePass/pppoeIdleTime/pppoeRedialPeriod/Ipv6in4_PrefixLen/LocalIpv6/RemoteIpv4/LanIPv6_Prefix/LanPrefixLen/ipv6to4Relay/ipv6rdRelay/tunrd_PrefixLen/wan_UseLinkLocal/Ipv6StaticIp/Ipv6PrefixLen leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-8827 | CVE-2025 - A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 2025080... | A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This issue affects the function um_inspect_cross_band of the file /goform/RP_setBasicAuto. The manipulation of the argument staticGateway 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-2025-8825 | CVE-2025 - A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20... | A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This affects the function RP_setBasicAuto of the file /goform/RP_setBasicAuto. The manipulation of the argument staticIp/staticNetmask leads to os command 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-2025-8823 | CVE-2025 - A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 2025080... | A vulnerability was found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this vulnerability is the function setDeviceName of the file /goform/setDeviceName. The manipulation of the argument DeviceName leads to os command injection. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | 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. | | |
| CVE-2025-8821 | CVE-2025 - A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20... | A vulnerability was identified in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. This issue affects the function RP_setBasic of the file /goform/RP_setBasic. The manipulation of the argument bssid 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-2025-8818 | CVE-2025 - A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20... | A vulnerability has been found in Linksys RE6250, RE6300, RE6350, RE6500, RE7000 and RE9000 up to 20250801. Affected by this issue is the function setDFSSetting of the file /goform/setLan. The manipulation of the argument lanNetmask/lanIp leads to os command 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-2025-45512 | CVE-2025 - A lack of signature verification in the bootloader of DENX Software Engineering Das U-Boot (U-Boot) ... | A lack of signature verification in the bootloader of DENX Software Engineering Das U-Boot (U-Boot) v1.1.3 allows attackers to install crafted firmware files, leading to arbitrary code execution. | Patched by core rule | Y |
| CVE-2025-48074 | CVE-2025 - OpenEXR provides the specification and reference implementation of the EXR file format, an image sto... | OpenEXR provides the specification and reference implementation of the EXR file format, an image storage format for the motion picture industry. In version 3.3.2, applications trust unvalidated dataWindow size values from file headers, which can lead to excessive memory allocation and performance degradation when processing malicious files. This is fixed in version 3.3.3. | Patched by core rule | Y |
| CVE-2019-19144 | CVE-2025 - XML External Entity Injection vulnerability in Quantum DXi6702 2.3.0.3 (11449-53631 Build304) device... | XML External Entity Injection vulnerability in Quantum DXi6702 2.3.0.3 (11449-53631 Build304) devices via rest/Users?action=authenticate. | Patched by core rule | Y |
| CVE-2025-45619 | CVE-2025 - An issue in Aver PTC310UV2 firmware v.0.1.0000.59 allows a remote attacker to execute arbitrary code... | An issue in Aver PTC310UV2 firmware v.0.1.0000.59 allows a remote attacker to execute arbitrary code via the SendAction function | Patched by core rule | Y |
| CVE-2025-25692 | CVE-2025 - A PHAR deserialization vulnerability in the _getHeaders function of | A PHAR deserialization vulnerability in the _getHeaders function of PrestaShop v8.2.0 allows | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | PrestaShop v8.2.0 allows attacke... | attackers to execute arbitrary code via a crafted POST request. | | |
| CVE-2025-25691 | CVE-2025 - A PHAR deserialization vulnerability in the component /themes/import of PrestaShop v8.2.0 allows att... | A PHAR deserialization vulnerability in the component /themes/import of PrestaShop v8.2.0 allows attackers to execute arbitrary code via a crafted POST request. | Patched by core rule | Y |
| CVE-2025-8259 | CVE-2025 - A vulnerability, which was classified as critical, was found in Vaelsys 4.1.0. This affects the func... | A vulnerability, which was classified as critical, was found in Vaelsys 4.1.0. This affects the function execute_DataObjectProc of the file /grid/vgrid_server.php. The manipulation of the argument xajaxargs leads to os command 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 |

## Path Traversal Vulnerabilities

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-29420 | CVE-2025 - PerfreeBlog v4.0.11 has a directory traversal vulnerability in the getThemeFilesByName function.... | PerfreeBlog v4.0.11 has a directory traversal vulnerability in the getThemeFilesByName function. | Patched by core rule | Y |
| CVE-2025-8562 | CVE-2025 - The Custom Query Shortcode plugin for WordPress is vulnerable to Path Traversal in all versions up t... | The Custom Query Shortcode plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 0.4.0 via the 'lens' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the contents of files on the server, which can contain sensitive information. | Patched by core rule | Y |
| CVE-2025-48303 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Kevin Langley Jr. Post Type Converter allows Cros... | Cross-Site Request Forgery (CSRF) vulnerability in Kevin Langley Jr. Post Type Converter allows Cross-Site Request Forgery.This issue affects Post Type Converter: from n/a through 0.6. | Patched by core rule | Y |
| CVE-2025-7839 | CVE-2025 - The Restore Permanently delete Post or Page Data plugin for WordPress is vulnerable to Cross-Site Re... | The Restore Permanently delete Post or Page Data plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on the rp_dpo_dpa_ajax_dp_delete_data() function. This makes it possible for unauthenticated attackers to delete data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |
| CVE-2025-57895 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Hossni Mubarak JobWP allows Cross Site Request Fo... | Cross-Site Request Forgery (CSRF) vulnerability in Hossni Mubarak JobWP allows Cross Site Request Forgery. This issue affects JobWP: from n/a through 2.4.3. | Patched by core rule | Y |
| CVE-2025-57893 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Epsiloncool WP Fast Total Search allows Cross Sit... | Cross-Site Request Forgery (CSRF) vulnerability in Epsiloncool WP Fast Total Search allows Cross Site Request Forgery. This issue affects WP Fast Total Search: from n/a through 1.79.270. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-57892 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Jeff Starr Simple Statistics for Feeds allows Cro... | Cross-Site Request Forgery (CSRF) vulnerability in Jeff Starr Simple Statistics for Feeds allows Cross Site Request Forgery. This issue affects Simple Statistics for Feeds: from n/a through 20250322. | Patched by core rule | Y |
| CVE-2025-57885 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Shahjahan Jewel Fluent Support allows Cross Site ... | Cross-Site Request Forgery (CSRF) vulnerability in Shahjahan Jewel Fluent Support allows Cross Site Request Forgery. This issue affects Fluent Support: from n/a through 1.9.1. | Patched by core rule | Y |
| CVE-2025-8895 | CVE-2025 - The WP Webhooks plugin for WordPress is vulnerable to arbitrary file copy due to missing validation ... | The WP Webhooks plugin for WordPress is vulnerable to arbitrary file copy due to missing validation of user-supplied input in all versions up to, and including, 3.3.5. This makes it possible for unauthenticated attackers to copy arbitrary files on the affected site's server to arbitrary locations. This can be used to copy the contents of wp-config.php into a text file which can then be accessed in a browser to reveal database credentials. | Patched by core rule | Y |
| CVE-2025-43748 | CVE-2025 - Insufficient CSRF protection for omni-administrator users in Liferay Portal 7.0.0 through 7.4.3.119,... | Insufficient CSRF protection for omni-administrator users in Liferay Portal 7.0.0 through 7.4.3.119, and Liferay DXP 2024.Q1.1 through 2024.Q1.6, 2023.Q4.0 through 2023.Q4.9, 2023.Q3.1 through 2023.Q3.9, 7.4 GA through update 92, 7.3 GA through update 36, and older unsupported versions allows attackers to execute Cross-Site Request Forgery | Patched by core rule | Y |
| CVE-2025-8102 | CVE-2025 - The Easy Digital Downloads plugin for WordPress is vulnerable to Cross-Site Request Forgery in all v... | The Easy Digital Downloads plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.5.0. This is due to missing nonce validations in the edd_sendwp_disconnect() and edd_sendwp_remote_install() functions. This makes it possible for unauthenticated attackers to deactivate or download and activate the SendWP | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | | |
| CVE-2025-54052 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Realtyna Realtyna Organic IDX plugin allows PHP L... | Cross-Site Request Forgery (CSRF) vulnerability in Realtyna Realtyna Organic IDX plugin allows PHP Local File Inclusion. This issue affects Realtyna Organic IDX plugin: from n/a through 5.0.0. | Patched by core rule | Y |
| CVE-2025-54021 | CVE-2025 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mitc... | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mitchell Bennis Simple File List allows Path Traversal. This issue affects Simple File List: from n/a through 6.1.14. | Patched by core rule | Y |
| CVE-2025-53561 | CVE-2025 - Path Traversal vulnerability in miniOrange Prevent files / folders access allows Path Traversal. Thi... | Path Traversal vulnerability in miniOrange Prevent files / folders access allows Path Traversal. This issue affects Prevent files / folders access: from n/a through 2.6.0. | Patched by core rule | Y |
| CVE-2025-49896 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in wptasker WP Discord Post Plus – Supports U... | Cross-Site Request Forgery (CSRF) vulnerability in wptasker WP Discord Post Plus – Supports Unlimited Channels allows Cross Site Request Forgery. This issue affects WP Discord Post Plus – Supports Unlimited Channels: from n/a through 1.0.2. | Patched by core rule | Y |
| CVE-2025-49426 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Dourou Cookie Warning allows Cross Site Request F... | Cross-Site Request Forgery (CSRF) vulnerability in Dourou Cookie Warning allows Cross Site Request Forgery. This issue affects Cookie Warning: from n/a through 1.3. | Patched by core rule | Y |
| CVE-2025-49399 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Basix NEX-Forms allows Cross Site Request Forgery... | Cross-Site Request Forgery (CSRF) vulnerability in Basix NEX-Forms allows Cross Site Request Forgery. This issue affects NEX-Forms: from n/a through 9.1.3. | Patched by core rule | Y |
| CVE-2025-49391 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Fetch Designs Sign-up Sheets allows Cross Site Re... | Cross-Site Request Forgery (CSRF) vulnerability in Fetch Designs Sign-up Sheets allows Cross Site Request Forgery. This issue affects Sign-up Sheets: from n/a through 2.3.3. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-49382 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in DexignZone JobZilla - Job Board WordPress Theme a... | Cross-Site Request Forgery (CSRF) vulnerability in DexignZone JobZilla - Job Board WordPress Theme allows Privilege Escalation. This issue affects JobZilla - Job Board WordPress Theme: from n/a through 2.0. | Patched by core rule | Y |
| CVE-2025-49381 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in ads.txt Guru ads.txt Guru Connect allows Cross Si... | Cross-Site Request Forgery (CSRF) vulnerability in ads.txt Guru ads.txt Guru Connect allows Cross Site Request Forgery. This issue affects ads.txt Guru Connect: from n/a through 1.1.1. | Patched by core rule | Y |
| CVE-2025-48158 | CVE-2025 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Alex... | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Alex Githatu BuddyPress XProfile Custom Image Field allows Path Traversal. This issue affects BuddyPress XProfile Custom Image Field: from n/a through 3.0.1. | Patched by core rule | Y |
| CVE-2025-47650 | CVE-2025 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Infi... | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Infility Infility Global allows Path Traversal. This issue affects Infility Global: from n/a through 2.14.7. | Patched by core rule | Y |
| CVE-2025-8141 | CVE-2025 - The Redirection for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file deletion due... | The Redirection for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_associated_files function in all versions up to, and including, 3.2.4. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). | Patched by core rule | Y |
| CVE-2025-43745 | CVE-2025 - A CSRF vulnerability in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 20... | A CSRF vulnerability in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.7, 2025.Q1.0 through 2025.Q1.14, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | 2024.Q1.1 through 2024.Q1.19 and 7.4 GA through update 92 allows remote attackers to performs cross-origin request on behalf of the authenticated user via the endpoint parameter. | | |
| CVE-2025-8464 | CVE-2025 - The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to Dire... | The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.3.9.0 via the wpcf7_guest_user_id cookie. This makes it possible for unauthenticated attackers to upload and delete files outside of the originally intended directory. The impact of this vulnerability is limited, as file types are validated and only safe ones can be uploaded, while deletion is limited to the plugin's uploads folder. | Patched by core rule | Y |
| CVE-2025-7686 | CVE-2025 - The weichuncai(WP伪春菜) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versio... | The weichuncai(WP伪春菜) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5. This is due to missing or incorrect nonce validation on the sm-options.php page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |
| CVE-2025-7684 | CVE-2025 - The Last.fm Recent Album Artwork plugin for WordPress is vulnerable to Cross-Site Request Forgery in... | The Last.fm Recent Album Artwork plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.2. This is due to missing or incorrect nonce validation on the 'lastfm_albums_artwork.php' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-7683 | CVE-2025 - The LatestCheckins plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions ... | The LatestCheckins plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1. This is due to missing or incorrect nonce validation on the 'LatestCheckins' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |
| CVE-2025-7668 | CVE-2025 - The Linux Promotional Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all... | The Linux Promotional Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to missing or incorrect nonce validation on the 'inux-promotional-plugin.php' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |
| CVE-2025-49895 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in iThemes ServerBuddy by PluginBuddy.Com allows Obj... | Cross-Site Request Forgery (CSRF) vulnerability in iThemes ServerBuddy by PluginBuddy.Com allows Object Injection.This issue affects ServerBuddy by PluginBuddy.Com: from n/a through 1.0.5. | Patched by core rule | Y |
| CVE-2025-7688 | CVE-2025 - The Add User Meta plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions u... | The Add User Meta plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on the 'add-user-meta' page. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-7641 | CVE-2025 - The Assistant for NextGEN Gallery plugin for WordPress is vulnerable to arbitrary directory deletion... | The Assistant for NextGEN Gallery plugin for WordPress is vulnerable to arbitrary directory deletion due to insufficient file path validation in the /wp-json/nextgenassistant/v1.0.0/control REST endpoint in all versions up to, and including, 1.0.9. This makes it possible for unauthenticated attackers to delete arbitrary directories on the server, which can cause a complete loss of availability. | Patched by core rule | Y |
| CVE-2025-54732 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Shahjada WPDM – Premium Packages allows Cross Sit... | Cross-Site Request Forgery (CSRF) vulnerability in Shahjada WPDM – Premium Packages allows Cross Site Request Forgery. This issue affects WPDM – Premium Packages: from n/a through 6.0.2. | Patched by core rule | Y |
| CVE-2025-54728 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in CreativeMindsSolutions CM On Demand Search And Re... | Cross-Site Request Forgery (CSRF) vulnerability in CreativeMindsSolutions CM On Demand Search And Replace allows Cross Site Request Forgery. This issue affects CM On Demand Search And Replace: from n/a through 1.5.2. | Patched by core rule | Y |
| CVE-2025-54715 | CVE-2025 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Dmit... | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Dmitry V. (CEO of "UKR Solution") Barcode Scanner with Inventory & Order Manager allows Path Traversal. This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.9.0. | Patched by core rule | Y |
| CVE-2025-53587 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in ApusTheme Findgo allows Cross Site Request Forger... | Cross-Site Request Forgery (CSRF) vulnerability in ApusTheme Findgo allows Cross Site Request Forgery. This issue affects Findgo: from n/a through 1.3.57. | Patched by core rule | Y |
| CVE-2025-53347 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Laborator Kalium allows Cross Site Request Forger... | Cross-Site Request Forgery (CSRF) vulnerability in Laborator Kalium allows Cross Site Request Forgery. This issue affects Kalium: from n/a through 3.18.3. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-53249 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in hakeemnala Build App Online allows Cross Site Req... | Cross-Site Request Forgery (CSRF) vulnerability in hakeemnala Build App Online allows Cross Site Request Forgery. This issue affects Build App Online: from n/a through 1.0.23. | Patched by core rule | Y |
| CVE-2025-53219 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in pl4g4 WP-Database-Optimizer-Tools allows Cross Si... | Cross-Site Request Forgery (CSRF) vulnerability in pl4g4 WP-Database-Optimizer-Tools allows Cross Site Request Forgery. This issue affects WP-Database-Optimizer-Tools: from n/a through 0.2. | Patched by core rule | Y |
| CVE-2025-52797 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in josepsitjar StoryMap allows SQL Injection. This i... | Cross-Site Request Forgery (CSRF) vulnerability in josepsitjar StoryMap allows SQL Injection. This issue affects StoryMap: from n/a through 2.1. | Patched by core rule | Y |
| CVE-2025-52769 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in flexostudio flexo-social-gallery allows Cross Sit... | Cross-Site Request Forgery (CSRF) vulnerability in flexostudio flexo-social-gallery allows Cross Site Request Forgery. This issue affects flexo-social-gallery: from n/a through 1.0006. | Patched by core rule | Y |
| CVE-2025-52767 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in lisensee NetInsight Analytics Implementation Plug... | Cross-Site Request Forgery (CSRF) vulnerability in lisensee NetInsight Analytics Implementation Plugin allows Cross Site Request Forgery. This issue affects NetInsight Analytics Implementation Plugin: from n/a through 1.0.3. | Patched by core rule | Y |
| CVE-2025-52765 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in lisensee NetInsight Analytics Implementation Plug... | Cross-Site Request Forgery (CSRF) vulnerability in lisensee NetInsight Analytics Implementation Plugin allows Stored XSS. This issue affects NetInsight Analytics Implementation Plugin: from n/a through 1.0.3. | Patched by core rule | Y |
| CVE-2024-53946 | CVE-2025 - The KuWFi 4G LTE AC900 router 1.0.13 is vulnerable to Cross-Site Request Forgery (CSRF) on its web m... | The KuWFi 4G LTE AC900 router 1.0.13 is vulnerable to Cross-Site Request Forgery (CSRF) on its web management interface. This vulnerability allows an attacker to trick an authenticated admin user into performing unauthorized actions, such as exploiting a command injection vulnerability in /goform/formMultiApnSetting. Successful exploitation can also lead to unauthorized configuration changes. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-54703 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Prince Integrate Google Drive allows Cross Site R... | Cross-Site Request Forgery (CSRF) vulnerability in Prince Integrate Google Drive allows Cross Site Request Forgery. This issue affects Integrate Google Drive: from n/a through 1.5.2. | Patched by core rule | Y |
| CVE-2025-54702 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in motov.net Ebook Store allows Cross Site Request F... | Cross-Site Request Forgery (CSRF) vulnerability in motov.net Ebook Store allows Cross Site Request Forgery. This issue affects Ebook Store: from n/a through 5.8013. | Patched by core rule | Y |
| CVE-2025-54694 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in bPlugins Button Block allows Cross Site Request F... | Cross-Site Request Forgery (CSRF) vulnerability in bPlugins Button Block allows Cross Site Request Forgery. This issue affects Button Block: from n/a through 1.2.0. | Patched by core rule | Y |
| CVE-2025-54682 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in CRM Perks Connector for Gravity Forms and Google ... | Cross-Site Request Forgery (CSRF) vulnerability in CRM Perks Connector for Gravity Forms and Google Sheets allows Cross Site Request Forgery. This issue affects Connector for Gravity Forms and Google Sheets: from n/a through 1.2.4. | Patched by core rule | Y |
| CVE-2025-54675 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in YITHEMES YITH WooCommerce Popup allows Cross Site... | Cross-Site Request Forgery (CSRF) vulnerability in YITHEMES YITH WooCommerce Popup allows Cross Site Request Forgery. This issue affects YITH WooCommerce Popup: from n/a through 1.48.0. | Patched by core rule | Y |
| CVE-2025-54674 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in mklacroix Product Configurator for WooCommerce al... | Cross-Site Request Forgery (CSRF) vulnerability in mklacroix Product Configurator for WooCommerce allows Cross Site Request Forgery. This issue affects Product Configurator for WooCommerce: from n/a through 1.4.4. | Patched by core rule | Y |
| CVE-2025-54673 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Chartify allows Cross Site Request Forger... | Cross-Site Request Forgery (CSRF) vulnerability in Ays Pro Chartify allows Cross Site Request Forgery. This issue affects Chartify: from n/a through 3.5.3. | Patched by core rule | Y |
| CVE-2025-54672 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in Jordy Meow Photo Engine allows Cross Site Request... | Cross-Site Request Forgery (CSRF) vulnerability in Jordy Meow Photo Engine allows Cross Site Request Forgery. This issue affects Photo Engine: from n/a | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | through 6.4.3. | | |
| CVE-2025-54671 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in bobbingwide oik allows Cross Site Request Forgery... | Cross-Site Request Forgery (CSRF) vulnerability in bobbingwide oik allows Cross Site Request Forgery. This issue affects oik: from n/a through 4.15.2. | Patched by core rule | Y |
| CVE-2025-52712 | CVE-2025 - Path Traversal vulnerability in BoldGrid Post and Page Builder by BoldGrid – Visual Drag and Drop Ed... | Path Traversal vulnerability in BoldGrid Post and Page Builder by BoldGrid – Visual Drag and Drop Editor allows Path Traversal. This issue affects Post and Page Builder by BoldGrid – Visual Drag and Drop Editor: from n/a through 1.27.8. | Patched by core rule | Y |
| CVE-2025-49044 | CVE-2025 - Cross-Site Request Forgery (CSRF) vulnerability in tosend.it Simple Poll allows Stored XSS. This iss... | Cross-Site Request Forgery (CSRF) vulnerability in tosend.it Simple Poll allows Stored XSS. This issue affects Simple Poll: from n/a through 1.1.1. | Patched by core rule | Y |
| CVE-2025-34154 | CVE-2025 - UnForm Server Manager versions prior to 10.1.12 expose an unauthenticated file read vulnerability vi... | UnForm Server Manager versions prior to 10.1.12 expose an unauthenticated file read vulnerability via its log file analysis interface. The flaw resides in the arc endpoint, which accepts a fl parameter to specify the log file to be opened. Due to insufficient input validation and lack of path sanitization, attackers can supply relative paths to access arbitrary files on the host system — including sensitive OS-level files — without authentication. | Patched by core rule | Y |
| CVE-2025-8491 | CVE-2025 - The Easy restaurant menu manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in... | The Easy restaurant menu manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.2. This is due to missing or incorrect nonce validation on the nsc_eprm_save_menu() function. This makes it possible for unauthenticated attackers to upload a menu file via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-0818 | CVE-2025 - Several WordPress plugins using elFinder versions 2.1.64 and prior are vulnerable to Directory Trave... | Several WordPress plugins using elFinder versions 2.1.64 and prior are vulnerable to Directory Traversal in various versions. This makes it possible for unauthenticated attackers to delete arbitrary files. Successful exploitation of this vulnerability requires a site owner to explicitly make an instance of the file manager available to users. | Patched by core rule | Y |
| CVE-2025-8081 | CVE-2025 - The Elementor plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and i... | The Elementor plugin for WordPress is vulnerable to Arbitrary File Read in all versions up to, and including, 3.30.2 via the Import_Images::import() function due to insufficient controls on the filename specified. 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-2025-5391 | CVE-2025 - The WooCommerce Purchase Orders plugin for WordPress is vulnerable to arbitrary file deletion due to... | The WooCommerce Purchase Orders plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_file() function in all versions up to, and including, 1.0.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). | Patched by core rule | Y |
| CVE-2024-55401 | CVE-2025 - An issue in 4C Strategies Exonaut before v22.4 allows attackers to execute a directory traversal.... | An issue in 4C Strategies Exonaut before v22.4 allows attackers to execute a directory traversal. | Patched by core rule | Y |
| CVE-2025-8505 | CVE-2025 - A vulnerability has been found in 495300897 wx-shop up to de1b66331368695779cfc6e4d11a64caddf8716e a... | A vulnerability has been found in 495300897 wx-shop up to de1b66331368695779cfc6e4d11a64caddf8716e and classified as problematic. This vulnerability affects unknown code. The manipulation leads to | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | cross-site request forgery. The attack can be initiated 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. | | |
| CVE-2025-50847 | CVE-2025 - Cross Site Request Forgery (CSRF) vulnerability in CS Cart 4.18.3, allows attackers to add products ... | Cross Site Request Forgery (CSRF) vulnerability in CS Cart 4.18.3, allows attackers to add products to a user's comparison list via a crafted HTTP request. | Patched by core rule | Y |
| CVE-2025-8151 | CVE-2025 - The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Path Traversal in ... | The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 2.9.1 via the 'save_block_css' function. This makes it possible for authenticated attackers, with Author-level access and above, to create CSS files in any directory, and delete CSS files in any directory in a Windows environment. | Patched by core rule | Y |
| CVE-2025-44137 | CVE-2025 - MapTiler Tileserver-php v2.0 is vulnerable to Directory Traversal. The renderTile function within ti... | MapTiler Tileserver-php v2.0 is vulnerable to Directory Traversal. The renderTile function within tileserver.php is responsible for delivering tiles that are stored as files on the server via web request. Creating the path to a file allows the insertion of "../" and thus read any file on the web server. Affected GET parameters are "TileMatrix", "TileRow", "TileCol" and "Format" | Patched by core rule | Y |
| CVE-2025-8223 | CVE-2025 - A vulnerability, which was classified as problematic, was found in jerryshensjf JPACookieShop 蛋糕商城 JP... | A vulnerability, which was classified as problematic, was found in jerryshensjf JPACookieShop 蛋糕商城 JPA版 up to 24a15c02b4f75042c9f7f615a3fed2ec1cefb999. This affects an unknown part of the file AdminTypeCustController.java. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. | | |
| CVE-2025-8104 | CVE-2025 - The Memory Usage plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up... | The Memory Usage plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.98. This is due to missing nonce validation in the wpmemory_install_plugin( ) function. This makes it possible for unauthenticated attackers to silently install one of the several whitelisted plugins via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |
| CVE-2025-8103 | CVE-2025 - The WPeMatico RSS Feed Fetcher plugin for WordPress is vulnerable to Cross-Site Request Forgery in a... | The WPeMatico RSS Feed Fetcher plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.8.7. This is due to missing nonce validation in the handle_feedback_submissi on() function. This makes it possible for unauthenticated attackers to deactivate the plugin via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. | Patched by core rule | Y |

## Server-side Request Forgery Vulnerabilities

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-9414 | CVE-2025 - A vulnerability was found in kalcaddle kodbox 1.61. Affected by this vulnerability is an unknown fun... | A vulnerability was found in kalcaddle kodbox 1.61. Affected by this vulnerability is an unknown functionality of the file /?explorer/upload/serverDownload of the component Download from Link Handler. Performing manipulation of the argument url results in server-side request forgery. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2024-46413 | CVE-2025 - Rebuild v3.7.7 was discovered to contain a Server-Side Request Forgery (SSRF) via the type parameter... | Rebuild v3.7.7 was discovered to contain a Server-Side Request Forgery (SSRF) via the type parameter in the com.rebuild.web.admin.rbstore.RBStoreController#loadDataIndex method. | Patched by core rule | Y |
| CVE-2025-9402 | CVE-2025 - A vulnerability was found in HuangDou UTCMS 9. This issue affects some unknown processing of the fil... | A vulnerability was found in HuangDou UTCMS 9. This issue affects some unknown processing of the file app/modules/ut-frame/admin/update.php of the component Config Handler. Performing manipulation of the argument UPDATEURL results in server-side request forgery. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-9395 | CVE-2025 - A vulnerability was identified in wangsongyan wblog 0.0.1. This affects the function RestorePost of ... | A vulnerability was identified in wangsongyan wblog 0.0.1. This affects the function RestorePost of the file backup.go. Such manipulation of the argument fileName leads to server-side request forgery. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | respond in any way. | | |
| CVE-2025-7813 | CVE-2025 - The Events Calendar, Event Booking, Registrations and Event Tickets – Eventin plugin for WordPress i... | The Events Calendar, Event Booking, Registrations and Event Tickets – Eventin plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.0.37 via the proxy_image function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. | Patched by core rule | Y |
| CVE-2025-8678 | CVE-2025 - The WP Crontrol plugin for WordPress is vulnerable to Server-Side Request Forgery in versions 1.17.0... | The WP Crontrol plugin for WordPress is vulnerable to Server-Side Request Forgery in versions 1.17.0 to 1.19.1 via the 'wp_remote_request' function. 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 and can be used to query and modify information from internal services. | Patched by core rule | Y |
| CVE-2025-43747 | CVE-2025 - A server-side request forgery (SSRF) vulnerability exists in the Liferay DXP 2025.Q2.0 through 2025.... | A server-side request forgery (SSRF) vulnerability exists in the Liferay DXP 2025.Q2.0 through 2025.Q2.3 due to insecure domain validation on analytics.cloud.domain.allowed, allowing an attacker to perform requests by change the domain and bypassing the validation method, this insecure validation is not distinguishing between trusted subdomains and malicious domains. | Patched by core rule | Y |
| CVE-2025-8013 | CVE-2025 - The Quttera Web Malware Scanner plugin for WordPress is vulnerable to Server-Side Request Forgery in... | The Quttera Web Malware Scanner plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.5.1.41 via the 'RunExternalScan' function. 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 and can be used to query and modify | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | information from internal services. | | |
| CVE-2025-8680 | CVE-2025 - The B Slider-Gutenberg Slider Block for WP plugin for WordPress is vulnerable to Server-Side Reques... | The B Slider- Gutenberg Slider Block for WP plugin for WordPress is vulnerable to Server-Side Request Forgery in version less than, or equal to, 2.0.0 via the fs_api_request function. This makes it possible for authenticated attackers, with subscriber-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-2025-53241 | CVE-2025 - Server-Side Request Forgery (SSRF) vulnerability in kodeshpa Simplified allows Server Side Request F... | Server-Side Request Forgery (SSRF) vulnerability in kodeshpa Simplified allows Server Side Request Forgery. This issue affects Simplified: from n/a through 1.0.9. | Patched by core rule | Y |
| CVE-2025-28987 | CVE-2025 - Server-Side Request Forgery (SSRF) vulnerability in PressForward PressForward allows Server Side Req... | Server-Side Request Forgery (SSRF) vulnerability in PressForward PressForward allows Server Side Request Forgery. This issue affects PressForward: from n/a through 5.9.1. | Patched by core rule | Y |
| CVE-2025-4655 | CVE-2025 - SSRF vulnerability in FreeMarker templates in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DX... | SSRF vulnerability in FreeMarker templates in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.5, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15, 7.4 GA through update 92 allows template editors to bypass access validations via crafted URLs. | Patched by core rule | Y |
| CVE-2025-4581 | CVE-2025 - Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4 ,2024.Q4.0 throu... | Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4 ,2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15, 7.4 GA through update 92 allows a pre-authentication blind SSRF vulnerability in the portal-settings-authentication-opensso-web due to improper validation of user-supplied URLs. An attacker can exploit this issue to force | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | the server to make arbitrary HTTP requests to internal systems, potentially leading to internal network enumeration or further exploitation. | | |
| CVE-2024-55399 | CVE-2025 - 4C Strategies Exonaut before v21.6.2.1-1 was discovered to contain a Server-Side Request Forgery (SS... | 4C Strategies Exonaut before v21.6.2.1-1 was discovered to contain a Server-Side Request Forgery (SSRF). | Patched by core rule | Y |
| CVE-2025-50234 | CVE-2025 - MCCMS v2.7.0 has an SSRF vulnerability located in the index() method of the sys\apps\controllers\api... | MCCMS v2.7.0 has an SSRF vulnerability located in the index() method of the sys\apps\controllers\api\Gf.php file, where the pic parameter is processed. The pic parameter is decrypted using the sys_auth($pic, 1) function, which utilizes a hard-coded key Mc_Encryption_Key (bD2voYwPpNuJ7B8), defined in the db.php file. The decrypted URL is passed to the geturl() method, which uses cURL to make a request to the URL without proper security checks. An attacker can craft a malicious encrypted pic parameter, which, when decrypted, points to internal addresses or local file paths (such as http://127.0.0.1 or file:///). By using the file:// protocol, the attacker can access arbitrary files on the local file system (e.g., file:///etc/passwd, file:///C:/Windows/System32/drivers/etc/hosts), allowing them to read sensitive configuration files, log files, and more, leading to information leakage or system exposure. The danger of this SSRF vulnerability includes accessing internal services and local file systems through protocols like http://, ftp://, and file://, which can result in sensitive data leakage, remote code execution, privilege escalation, or full system compromise, severely affecting the system's security and stability. | Patched by core rule | Y |
| CVE-2025-8267 | CVE-2025 - Versions of the package ssrfcheck before 1.2.0 are vulnerable to Server-Side Request Forgery (SSRF) ... | Versions of the package ssrfcheck before 1.2.0 are vulnerable to Server-Side Request Forgery (SSRF) due to an incomplete denylist of | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | IP address ranges. Specifically, the package fails to classify the reserved IP address space 224.0.0.0/4 (Multicast) as invalid. This oversight allows attackers to craft requests targeting these multicast addresses. | | |

## SQL Injection Vulnerabilities

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-55575 | CVE-2025 - SQL Injection vulnerability in SMM Panel 3.1 allowing remote attackers to gain sensitive information... | SQL Injection vulnerability in SMM Panel 3.1 allowing remote attackers to gain sensitive information via a crafted HTTP request with action=service_detail. | Patched by core rule | Y |
| CVE-2025-9399 | CVE-2025 - A vulnerability was detected in YiFang CMS up to 2.0.5. Affected by this issue is some unknown funct... | A vulnerability was detected in YiFang CMS up to 2.0.5. Affected by this issue is some unknown functionality of the file app/logic/L_tool.php. The manipulation of the argument new_url results in sql injection. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-9238 | CVE-2025 - A vulnerability was determined in Swatadru Exam-Seating-Arrangement up to 97335ccebf95468d92525f4255... | A vulnerability was determined in Swatadru Exam-Seating-Arrangement up to 97335ccebf95468d92525f4255a2241d2b0b002f. Affected is an unknown function of the file /student.php of the component Student Login. Executing manipulation of the argument email can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-9236 | CVE-2025 - A vulnerability has been found in Portabilis i-Educar up to 2.10. This affects an unknown function o... | A vulnerability has been found in Portabilis i-Educar up to 2.10. This affects an unknown function of the file /intranet/educar_tipo_usuario_lst.php of the component Tipos de usuàrio Page. Such manipulation of the argument nm_tipo/descrição leads to sql injection. The attack may be performed from a remote location. The exploit has been disclosed to the public and may be used. The | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | vendor was contacted early about this disclosure but did not respond in any way. | | |
| CVE-2025-54726 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Miguel Useche JS Archive List allows SQL Injection. This issue affects JS Archive List: from n/a through n/a. | Patched by core rule | Y |
| CVE-2025-54048 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in miniOrange Custom API for WP allows SQL Injection. This issue affects Custom API for WP: from n/a through 4.2.2. | Patched by core rule | Y |
| CVE-2025-9149 | CVE-2025 - A vulnerability was determined in Wavlink WL-NU516U1 M16U1_V240425. This impacts the function sub_40... | A vulnerability was determined in Wavlink WL-NU516U1 M16U1_V240425. This impacts the function sub_4032E4 of the file /cgi-bin/wireless.cgi. This manipulation of the argument Guest_ssid causes command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. | Patched by core rule | Y |
| CVE-2025-51506 | CVE-2025 - In the smartLibrary component of the HRForecast Suite 0.4.3, a SQL injection vulnerability was disco... | In the smartLibrary component of the HRForecast Suite 0.4.3, a SQL injection vulnerability was discovered in the valueKey parameter. This flaw enables any authenticated user to execute arbitrary SQL queries, via crafted payloads to valueKey to the api/smartlibrary/v2/en/dictionaries/options/lookup endpoint. | Patched by core rule | Y |
| CVE-2025-50567 | CVE-2025 - Saurus CMS Community Edition 4.7.1 contains a vulnerability in the custom DB::prepare() function, wh... | Saurus CMS Community Edition 4.7.1 contains a vulnerability in the custom DB::prepare() function, which uses preg_replace() with the deprecated /e (eval) modifier to interpolate SQL query parameters. This leads to injection of user-controlled SQL statements, potentially leading to arbitrary PHP code execution. | Patched by core rule | Y |
| CVE-2025-7670 | CVE-2025 - The JS Archive List plugin for WordPress is vulnerable to time- | The JS Archive List plugin for WordPress is vulnerable to time-based SQL Injection via | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | based SQL Injection via the build_sql... | the build_sql_where() function in all versions up to, and including, 6.1.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. | | |
| CVE-2025-9090 | CVE-2025 - A vulnerability was identified in Tenda AC20 16.03.08.12. Affected is the function websFormDefine of... | A vulnerability was identified in Tenda AC20 16.03.08.12. Affected is the function websFormDefine of the file /goform/telnet of the component Telnet Service. The manipulation leads to command 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-2025-49897 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in gopiplus Vertical scroll slideshow gallery v2 allows Blind SQL Injection. This issue affects Vertical scroll slideshow gallery v2: from n/a through 9.1. | Patched by core rule | Y |
| CVE-2025-54475 | CVE-2025 - A SQL injection vulnerability in the JS Jobs plugin versions 1.3.2-1.4.4 for Joomla allows low-privi... | A SQL injection vulnerability in the JS Jobs plugin versions 1.3.2-1.4.4 for Joomla allows low-privilege users to execute arbitrary SQL commands. | Patched by core rule | Y |
| CVE-2025-7662 | CVE-2025 - The Gestion de tarifs plugin for WordPress is vulnerable to SQL Injection via the 'tarif' and 'intit... | The Gestion de tarifs plugin for WordPress is vulnerable to SQL Injection via the 'tarif' and 'intitule' shortcodes in all versions up to, and including, 1.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. | Patched by core rule | Y |
| CVE-2025-55708 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL | 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 |
|---|---|---|---|---|
| | Injection') vulnerability i... | ExpressTech Systems Quiz And Survey Master allows SQL Injection. This issue affects Quiz And Survey Master: from n/a through 10.2.4. | | |
| CVE-2025-54707 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RealMag777 MDTF allows SQL Injection. This issue affects MDTF: from n/a through 1.3.3.7. | Patched by core rule | Y |
| CVE-2025-54678 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in hassantafreshi Easy Form Builder allows Blind SQL Injection. This issue affects Easy Form Builder: from n/a through 3.8.15. | Patched by core rule | Y |
| CVE-2025-54669 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RomanCode MapSVG allows SQL Injection. This issue affects MapSVG: from n/a through n/a. | Patched by core rule | Y |
| CVE-2025-52823 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ovatheme Cube Portfolio allows SQL Injection. This issue affects Cube Portfolio: from n/a through 1.16.8. | Patched by core rule | Y |
| CVE-2025-52820 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in infosoftplugin WooCommerce Point Of Sale (POS) allows SQL Injection. This issue affects WooCommerce Point Of Sale (POS): from n/a through 1.4. | Patched by core rule | Y |
| CVE-2025-52720 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in highwarden Super Store Finder allows SQL Injection. This issue affects Super Store Finder: from n/a through 7.5. | Patched by core rule | Y |
| CVE-2025-49267 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Shabti Kaplan Frontend Admin by DynamiApps | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | allows Blind SQL Injection. This issue affects Frontend Admin by DynamiApps: from n/a through 3.28.3. | | |
| CVE-2025-49059 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CleverReach® CleverReach® WP allows SQL Injection. This issue affects CleverReach® WP: from n/a through 1.5.20. | Patched by core rule | Y |
| CVE-2025-49033 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Metagauss ProfileGrid allows Blind SQL Injection. This issue affects ProfileGrid : from n/a through 5.9.5.3. | Patched by core rule | Y |
| CVE-2025-39510 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ValvePress Pinterest Automatic Pin allows SQL Injection. This issue affects Pinterest Automatic Pin: from n/a through n/a. | Patched by core rule | Y |
| CVE-2025-30998 | CVE-2025 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability i... | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rico Macchi WP Links Page allows SQL Injection. This issue affects WP Links Page: from n/a through 4.9.6. | Patched by core rule | Y |
| CVE-2025-8956 | CVE-2025 - A vulnerability was found in D-Link DIR-818L up to 1.05B01. This issue affects the function getenv o... | A vulnerability was found in D-Link DIR-818L up to 1.05B01. This issue affects the function getenv of the file /htdocs/cgibin of the component ssdpcgi. The manipulation leads to command 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-2025-8937 | CVE-2025 - A vulnerability has been found in TOTOLINK N350R 1.2.3-B20130826. This vulnerability affects unknown... | A vulnerability has been found in TOTOLINK N350R 1.2.3-B20130826. This vulnerability affects unknown code of the file /boafrm/formSysCmd. The manipulation leads to command 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-2025-8908 | CVE-2025 - A vulnerability was | A vulnerability was determined in Shanghai | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | determined in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.5.... | Lingdang Information Technology Lingdang CRM up to 8.6.5.4. Affected by this issue is some unknown functionality of the file crm/WeiXinApp/yunzhijia/event.php. The manipulation of the argument openid 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 8.6.5 is able to address this issue. It is recommended to upgrade the affected component. The vendor explains: "All SQL injection vectors were patched via parameterized queries and input sanitization in v8.6.5+." | | |
| CVE-2024-32640 | CVE-2025 - MASA CMS is an Enterprise Content Management platform based on open source technology. Versions prio... | MASA CMS is an Enterprise Content Management platform based on open source technology. Versions prior to 7.4.6, 7.3.13, and 7.2.8 contain a SQL injection vulnerability in the `processAsyncObject` method that can result in remote code execution. Versions 7.4.6, 7.3.13, and 7.2.8 contain a fix for the issue. | Patched by core rule | Y |
| CVE-2025-8773 | CVE-2025 - A vulnerability, which was classified as critical, was found in Dinstar Monitoring Platform 甘肃省危险品库监... | A vulnerability, which was classified as critical, was found in Dinstar Monitoring Platform 甘肃省危险品库监控平台 1.0. Affected is an unknown function of the file /itc/$%7BappPath%7D/login_getPasswordErrorNum.action. The manipulation of the argument userBean.loginName 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-2025-50468 | CVE-2025 - OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the da... | OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the DocStoreDAO interface. The entityType parameters can be used to build a SQL query. | Patched by core rule | Y |
| CVE-2025-50467 | CVE-2025 - | OpenMetadata <=1.4.4 is | Patched by core | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the da... | vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the TestDefinitionDAO interface. The supportedDataTypeParam parameter can be used to build a SQL query. | rule | |
| CVE-2025-50466 | CVE-2025 - OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the da... | OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the TestDefinitionDAO interface. The entityType parameter can be used to build a SQL query. | Patched by core rule | Y |
| CVE-2025-50465 | CVE-2025 - OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the da... | OpenMetadata <=1.4.4 is vulnerable to SQL Injection. An attacker can extract information from the database in function listCount in the TestDefinitionDAO interface. The testPlatform parameter can be used to build a SQL query. | Patched by core rule | Y |
| CVE-2023-41532 | CVE-2025 - Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the doctor... | Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the doctor_contact parameter in doctorsearch.php. | Patched by core rule | Y |
| CVE-2023-41531 | CVE-2025 - Hospital Management System v4 was discovered to contain multiple SQL injection vulnerabilities in fu... | Hospital Management System v4 was discovered to contain multiple SQL injection vulnerabilities in func3.php via the username1 and password2 parameters. | Patched by core rule | Y |
| CVE-2023-41530 | CVE-2025 - Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the app_co... | Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the app_contact parameter in appsearch.php. | Patched by core rule | Y |
| CVE-2023-41528 | CVE-2025 - Hospital Management System v4 was discovered to contain multiple SQL injection vulnerabilities in co... | Hospital Management System v4 was discovered to contain multiple SQL injection vulnerabilities in contact.php via the txtname, txtphone, and txtmail parameters. | Patched by core rule | Y |
| CVE-2023-41527 | CVE-2025 - Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the passwo... | Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the password2 parameter in func.php. | Patched by core rule | Y |
| CVE-2023-41526 | CVE-2025 - Hospital | Hospital Management | Patched by core | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | Management System v4 was discovered to contain multiple SQL injection vulnerabilities in fu... | System v4 was discovered to contain multiple SQL injection vulnerabilities in func1.php via the username3 and password3 parameters. | rule | |
| CVE-2023-41525 | CVE-2025 - Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the patien... | Hospital Management System v4 was discovered to contain a SQL injection vulnerability via the patient_contact parameter in patientsearch.php. | Patched by core rule | Y |
| CVE-2023-41524 | CVE-2025 - Student Attendance Management System v1 was discovered to contain a SQL injection vulnerability via ... | Student Attendance Management System v1 was discovered to contain a SQL injection vulnerability via the username parameter at index.php. | Patched by core rule | Y |
| CVE-2023-41523 | CVE-2025 - Student Attendance Management System v1 was discovered to contain a SQL injection vulnerability via ... | Student Attendance Management System v1 was discovered to contain a SQL injection vulnerability via the emailAddress parameter at createClassTeacher.php. | Patched by core rule | Y |
| CVE-2023-41522 | CVE-2025 - Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabili... | Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabilities in createStudents.php via the Id, firstname, and admissionNumber parameters. | Patched by core rule | Y |
| CVE-2023-41521 | CVE-2025 - Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabili... | Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabilities in createSessionTerm.php via the id, termId, and sessionName parameters. | Patched by core rule | Y |
| CVE-2023-41520 | CVE-2025 - Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabili... | Student Attendance Management System v1 was discovered to contain multiple SQL injection vulnerabilities in createClassArms.php via the classId and classArmName parameters. | Patched by core rule | Y |
| CVE-2023-40992 | CVE-2025 - Hospital Management System 4 is vulnerable to a SQL injection in /Hospital-Management-System-master/... | Hospital Management System 4 is vulnerable to a SQL injection in /Hospital-Management-System-master/func.php via the password2 parameter. | Patched by core rule | Y |
| CVE-2025-7036 | CVE-2025 - The CleverReach® WP plugin for WordPress is vulnerable to time-based SQL Injection via the 'title' p... | The CleverReach® WP plugin for WordPress is vulnerable to time-based SQL Injection via the 'title' parameter in all versions up to, and including, 1.5.20 due to insufficient escaping on the user supplied parameter and | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | 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-2025-6986 | CVE-2025 - The FileBird – WordPress Media Library Folders & File Manager plugin for WordPress is vulnerable to ... | The FileBird – WordPress Media Library Folders & File Manager plugin for WordPress is vulnerable to SQL Injection via the 'search' parameter in all versions up to, and including, 6.4.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. | Patched by core rule | Y |
| CVE-2025-50341 | CVE-2025 - A Boolean-based SQL injection vulnerability was discovered in Axelor 5.2.4 via the _domain parameter... | A Boolean-based SQL injection vulnerability was discovered in Axelor 5.2.4 via the _domain parameter. An attacker can manipulate the SQL query logic and determine true/false conditions, potentially leading to data exposure or further exploitation. | Patched by core rule | Y |
| CVE-2025-8518 | CVE-2025 - A vulnerability was found in givanz Vvveb 1.0.5. It has been rated as critical. Affected by this iss... | A vulnerability was found in givanz Vvveb 1.0.5. It has been rated as critical. Affected by this issue is the function Save of the file admin/controller/editor/code.php of the component Code Editor. The manipulation leads to code injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.0.6 is able to address this issue. The name of the patch is f684f3e374d04db715730fc4796e102f5ebcacb2. It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2025-8500 | CVE-2025 - A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been rated a... | A vulnerability was found in code-projects Human Resource Integrated System 1.0. It has been rated as critical. This issue affects some unknown processing | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | of the file /insert-and-view/action.php. The manipulation of the argument content leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. | | |
| CVE-2025-8470 | CVE-2025 - A vulnerability classified as critical was found in SourceCodester Online Hotel Reservation System 1... | A vulnerability classified as critical was found in SourceCodester Online Hotel Reservation System 1.0. This vulnerability affects unknown code of the file /admin/deleteroom.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-2025-8469 | CVE-2025 - A vulnerability classified as critical has been found in SourceCodester Online Hotel Reservation Sys... | A vulnerability classified as critical has been found in SourceCodester Online Hotel Reservation System 1.0. This affects an unknown part of the file /admin/deletegallery.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-2025-50868 | CVE-2025 - A SQL Injection vulnerability exists in the takeassessment2.php file of CloudClassroom-PHP-Project 1... | A SQL Injection vulnerability exists in the takeassessment2.php file of CloudClassroom-PHP-Project 1.0. The Q4 POST parameter is not properly sanitized before being used in SQL queries. | Patched by core rule | Y |
| CVE-2025-52390 | CVE-2025 - Saurus CMS Community Edition since commit d886e5b0 (2010-04-23) is vulnerable to a SQL Injection vul... | Saurus CMS Community Edition since commit d886e5b0 (2010-04-23) is vulnerable to a SQL Injection vulnerability in the `prepareSearchQuery()` method in `FulltextSearch.class.php`. The application directly concatenates user-supplied input (`$search_word`) into SQL queries without sanitization, allowing attackers to manipulate the SQL logic and potentially extract sensitive information or escalate their privileges. | Patched by core rule | Y |
| CVE-2025-52327 | CVE-2025 - SQL Injection vulnerability in Restaurant Order System 1.0 allows a local attacker to obtain sensiti... | SQL Injection vulnerability in Restaurant Order System 1.0 allows a local attacker to obtain sensitive information via the payment.php file | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2024-34327 | CVE-2025 - Sielox AnyWare v2.1.2 was discovered to contain a SQL injection vulnerability via the email address ... | Sielox AnyWare v2.1.2 was discovered to contain a SQL injection vulnerability via the email address field of the password reset form. | Patched by core rule | Y |
| CVE-2025-50867 | CVE-2025 - A SQL Injection vulnerability exists in the takeassessment2.php endpoint of the CloudClassroom-PHP-P... | A SQL Injection vulnerability exists in the takeassessment2.php endpoint of the CloudClassroom-PHP-Project 1.0, where the Q5 POST parameter is directly embedded in SQL statements without sanitization. | Patched by core rule | Y |
| CVE-2025-8347 | CVE-2025 - A vulnerability, which was classified as critical, was found in Kehua Charging Pile Cloud Platform 1... | A vulnerability, which was classified as critical, was found in Kehua Charging Pile Cloud Platform 1.0. This affects an unknown part of the file /sys/task/findAllTask. 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. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-8345 | CVE-2025 - A vulnerability classified as critical was found in Shanghai Lingdang Information Technology Lingdan... | A vulnerability classified as critical was found in Shanghai Lingdang Information Technology Lingdang CRM up to 8.6.4.7. Affected by this vulnerability is the function delete_user of the file crm/WeiXinApp/yunzhijia/yunzhijiaApi.php. The manipulation of the argument function leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 8.6.5.2 is able to address this issue. It is recommended to upgrade the affected component. | Patched by core rule | Y |
| CVE-2025-8339 | CVE-2025 - A vulnerability was found in code-projects Intern Membership Management System 1.0. It has been clas... | A vulnerability was found in code-projects Intern Membership Management System 1.0. It has been classified as critical. This affects an unknown part of the file /student_login.php. The manipulation of the argument user_name/password leads to sql injection. It is possible to initiate the attack remotely. The exploit has | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | been disclosed to the public and may be used. | | |
| CVE-2025-6348 | CVE-2025 - The Smart Slider 3 plugin for WordPress is vulnerable to time-based SQL Injection via the 'sliderid'... | The Smart Slider 3 plugin for WordPress is vulnerable to time-based SQL Injection via the 'sliderid' parameter in all versions up to, and including, 3.5.1.28 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, 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-2024-43018 | CVE-2025 - Piwigo 13.8.0 and below is vulnerable to SQL Injection in the parameters max_level and min_register.... | Piwigo 13.8.0 and below is vulnerable to SQL Injection in the parameters max_level and min_register. These parameters are used in ws_user_gerList function from file include\ws_functions\pwg.users.php and this same function is called by ws.php file at some point can be used for searching users in advanced way in /admin.php?page=user_list. | Patched by core rule | Y |
| CVE-2025-51970 | CVE-2025 - A SQL Injection vulnerability exists in the action.php endpoint of PuneethReddyHC Online Shopping Sy... | A SQL Injection vulnerability exists in the action.php endpoint of PuneethReddyHC Online Shopping System Advanced 1.0 due to improper sanitization of user-supplied input in the keyword POST parameter. | Patched by core rule | Y |
| CVE-2024-13507 | CVE-2025 - The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPre... | The GeoDirectory – WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to time-based SQL Injection via the dist parameter in all versions up to, and including, 2.8.97 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 |

## Cross-site Scripting Vulnerabilities

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-9422 | CVE-2025 - A vulnerability was found in oitcode samarium up to 0.9.6. This impacts an unknown function of the f... | A vulnerability was found in oitcode samarium up to 0.9.6. This impacts an unknown function of the file /dashboard/team of the component Team Image Handler. The manipulation results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used. | Patched by core rule | Y |
| CVE-2025-9416 | CVE-2025 - A security flaw has been discovered in oitcode samarium up to 0.9.6. This vulnerability affects unkn... | A security flaw has been discovered in oitcode samarium up to 0.9.6. This vulnerability affects unknown code of the file /cms/webpage/ of the component Pages Image Handler. The manipulation results in cross site scripting. The attack may be performed from a remote location. The exploit has been released to the public and may be exploited. | Patched by core rule | Y |
| CVE-2025-9404 | CVE-2025 - A vulnerability was identified in Scada-LTS up to 2.7.8.1. The affected element is an unknown functi... | A vulnerability was identified in Scada-LTS up to 2.7.8.1. The affected element is an unknown function of the file /pointHierarchySLTS of the component Folder Handler. The manipulation of the argument Title leads to cross site scripting. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. | Patched by core rule | Y |
| CVE-2025-9388 | CVE-2025 - A vulnerability was determined in Scada-LTS up to 2.7.8.1. This impacts an unknown function of the f... | A vulnerability was determined in Scada-LTS up to 2.7.8.1. This impacts an unknown function of the file watch_list.shtm. Executing manipulation of the argument Name can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. | Patched by core rule | Y |
| CVE-2025-8208 | CVE-2025 - The Spexo Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via... | The Spexo Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 1.0.23 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-9131 | CVE-2025 - The Ogulo – 360° Tour plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slu... | The Ogulo – 360° Tour plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'slug' parameter in all versions up to, and including, 1.0.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8062 | CVE-2025 - The WS Theme Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin... | The WS Theme Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ws_weather shortcode in all versions up to, and including, 2.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-7957 | CVE-2025 - The ShortcodeHub plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author_l... | The ShortcodeHub plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author_link_target' parameter in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-43765 | CVE-2025 - A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Lifer... | A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.13 and 7.4 GA through update 92 allows an remote non- | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | authenticated attacker to inject JavaScript into the text field from a web content. | | |
| CVE-2025-43769 | CVE-2025 - Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.131, and Lifer... | Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q3.1 through 2024.Q3.8, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows remote attackers to execute arbitrary web script or HTML via components tab. | Patched by core rule | Y |
| CVE-2025-43770 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.3, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the referer or FORWARD_URL using %00 in those parameters. | Patched by core rule | Y |
| CVE-2025-43761 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.4, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the frontend-editor-ckeditor-web/ckeditor/samples/old/ajax.html path | Patched by core rule | Y |
| CVE-2025-43760 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4, 2024.Q4.0 through 2024.Q4.6, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.20 and 7.4 GA through update 92 | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | allows an remote authenticated attacker to inject JavaScript into the PortalUtil.escapeRedirect | | |
| CVE-2025-50733 | CVE-2025 - NextChat contains a cross-site scripting (XSS) vulnerability in the HTMLPreview component of artifac... | NextChat contains a cross-site scripting (XSS) vulnerability in the HTMLPreview component of artifacts.tsx that allows attackers to execute arbitrary JavaScript code when HTML content is rendered in the AI chat interface. The vulnerability occurs because user-influenced HTML from AI responses is rendered in an iframe with 'allow-scripts' sandbox permission without proper sanitization. This can be exploited through specifically crafted prompts that cause the AI to generate malicious HTML/JavaScript code. When a user views the HTML preview, the injected JavaScript executes in the user's browser context, potentially allowing attackers to exfiltrate sensitive information (including API keys stored in localStorage), perform actions on behalf of the user, and steal session data. | Patched by core rule | Y |
| CVE-2025-55573 | CVE-2025 - QuantumNous new-api v.0.8.5.2 is vulnerable to Cross Site Scripting (XSS).... | QuantumNous new-api v.0.8.5.2 is vulnerable to Cross Site Scripting (XSS). | Patched by core rule | Y |
| CVE-2025-57891 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpecommerce Recurring PayPal Donations allows Stored XSS. This issue affects Recurring PayPal Donations: from n/a through 1.8. | Patched by core rule | Y |
| CVE-2025-57890 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pierre Lannoy Sessions allows Stored XSS. This issue affects Sessions: from n/a through 3.2.0. | Patched by core rule | Y |
| CVE-2025-57887 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobmonster allows Stored XSS. This issue affects Jobmonster: from n/a through 4.8.0. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-43753 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.32 through 7.4.3.13... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.32 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.7, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 update 32 through update 92 allows an remote authenticated user to inject JavaScript into the embedded message field from the form container. | Patched by core rule | Y |
| CVE-2025-51606 | CVE-2025 - hippo4j 1.0.0 to 1.5.0, uses a hard-coded secret key in its JWT (JSON Web Token) creation. This allo... | hippo4j 1.0.0 to 1.5.0, uses a hard-coded secret key in its JWT (JSON Web Token) creation. This allows attackers with access to the source code or compiled binary to forge valid access tokens and impersonate any user, including privileged ones such as "admin". The vulnerability poses a critical security risk in systems where authentication and authorization rely on the integrity of JWTs. | Patched by core rule | Y |
| CVE-2025-55522 | CVE-2025 - Cross-site scripting (XSS) vulnerability in the component /common/reports of Akaunting v3.1.18 allow... | Cross-site scripting (XSS) vulnerability in the component /common/reports of Akaunting v3.1.18 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the name parameter. | Patched by core rule | Y |
| CVE-2025-43756 | CVE-2025 - <!--td {border: 1px solid #cccccc;}br {mso-data-placement:same-cell;}-->A reflected cross-site scrip... | <!--td {border: 1px solid #cccccc;}br {mso-data-placement:same-cell;}-->A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.15, 2025.Q2.0 through 2025.Q2.2 and 2024.Q1.13 through 2024.Q1.19 allows a remote authenticated user to inject JavaScript code via snippet parameter. | Patched by core rule | Y |
| CVE-2025-43755 | CVE-2025 - A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 t through 7.4.3.132, and Lif... | A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 t through 7.4.3.132, and Liferay DXP 2025.Q2.0, 2025.Q1.0 through 2025.Q1.13, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.17 and 7.4 GA through update 92 allows an remote authenticated attacker to inject JavaScript into the _com_liferay_layout_admin_web_portlet_GroupPagesPortlet_type parameter. | | |
| CVE-2025-8064 | CVE-2025 - The Bible SuperSearch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sel... | The Bible SuperSearch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'selector_height' parameter in all versions up to, and including, 6.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8607 | CVE-2025 - The SlingBlocks – Gutenberg Blocks by FunnelKit (Formerly WooFunnels) plugin for WordPress is vulner... | The SlingBlocks – Gutenberg Blocks by FunnelKit (Formerly WooFunnels) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown block's attributes in all versions up to, and including, 1.6.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-43757 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.2, 2025.Q1.0 through 2025.Q1.14, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.18 and 7.4 GA through update 92 allows a remote authenticated attacker to inject JavaScript code via _com_liferay_dynamic_data | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | _mapping_web_portlet_DDMPortlet_definition parameter. | | |
| CVE-2025-43746 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.2, 2025.Q1.0 through 2025.Q1.14, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.18 and 7.4 GA through update 92 allows a remote authenticated attacker to inject JavaScript code via _com_liferay_dynamic_data_mapping_web_portlet_DDMPortlet_portletNamespace and _com_liferay_dynamic_data_mapping_web_portlet_DDMPortlet_namespace parameter. | Patched by core rule | Y |
| CVE-2025-9237 | CVE-2025 - A vulnerability was found in CodeAstro Ecommerce Website 1.0. This impacts an unknown function of th... | A vulnerability was found in CodeAstro Ecommerce Website 1.0. This impacts an unknown function of the file /customer/my_account.php ?edit_account of the component Edit Your Account Page. Performing manipulation of the argument Username results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. | Patched by core rule | Y |
| CVE-2025-9235 | CVE-2025 - A flaw has been found in Scada-LTS up to 2.7.8.1. The impacted element is an unknown function of the... | A flaw has been found in Scada-LTS up to 2.7.8.1. The impacted element is an unknown function of the file compound_events.shtm. This manipulation of the argument Name causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used. | Patched by core rule | Y |
| CVE-2025-9234 | CVE-2025 - A vulnerability was detected in Scada-LTS up to 2.7.8.1. The affected element is an unknown function... | A vulnerability was detected in Scada-LTS up to 2.7.8.1. The affected element is an unknown function of the file maintenance_events.shtm. The manipulation of the argument Alias results in cross site scripting. The attack can be executed | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | remotely. The exploit is now public and may be used. | | |
| CVE-2025-9233 | CVE-2025 - A security vulnerability has been detected in Scada-LTS up to 2.7.8.1. Impacted is an unknown functi... | A security vulnerability has been detected in Scada-LTS up to 2.7.8.1. Impacted is an unknown function of the file view_edit.shtm. The manipulation of the argument Name leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. | Patched by core rule | Y |
| CVE-2025-51991 | CVE-2025 - XWiki through version 17.3.0 is vulnerable to Server-Side Template Injection (SSTI) in the Administr... | XWiki through version 17.3.0 is vulnerable to Server-Side Template Injection (SSTI) in the Administration interface, specifically within the HTTP Meta Info field of the Global Preferences Presentation section. An authenticated administrator can inject crafted Apache Velocity template code, which is rendered on the server side without proper validation or sandboxing. This enables the execution of arbitrary template logic, which may expose internal server information or, in specific configurations, lead to further exploitation such as remote code execution or sensitive data leakage. The vulnerability resides in improper handling of dynamic template rendering within user-supplied configuration fields. | Patched by core rule | Y |
| CVE-2025-51990 | CVE-2025 - XWiki through version 17.3.0 is affected by multiple stored Cross-Site Scripting (XSS) vulnerabiliti... | XWiki through version 17.3.0 is affected by multiple stored Cross-Site Scripting (XSS) vulnerabilities in the Administration interface, specifically under the Presentation section of the Global Preferences panel. An authenticated administrator can inject arbitrary JavaScript payloads into the HTTP Meta Info, Footer Copyright, and Footer Version fields. These inputs are stored and subsequently rendered without proper output encoding or sanitization on public-facing pages. As a result, the injected scripts are persistently executed in the browser context of any visitor to the affected instances including both authenticated and | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | unauthenticated users. No user interaction is required beyond visiting a page that includes the malicious content. Successful exploitation can lead to session hijacking, credential theft, unauthorized actions via session riding, or further compromise of the application through client-side attacks. The vulnerability introduces significant risk in any deployment, especially in shared or internet-facing environments where administrator credentials may be compromised. | | |
| CVE-2025-43742 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.3, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript in web content for friendly urls. | Patched by core rule | Y |
| CVE-2025-43741 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.3, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.14 and 7.4 GA through update 92 allows an remote authenticated attacker to inject JavaScrip in the _com_liferay_users_admin_web_portlet_UsersAdminPortlet_assetTagNames parameter | Patched by core rule | Y |
| CVE-2025-54670 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bobbingwide oik allows Reflected XSS. This issue affects oik: from n/a through 4.15.2. | Patched by core rule | Y |
| CVE-2025-54056 | CVE-2025 - Improper | Improper Neutralization of | Patched by core | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Responsive HTML5 Audio Player PRO With Playlist allows Reflected XSS. This issue affects Responsive HTML5 Audio Player PRO With Playlist: from n/a through 3.5.8. | rule | |
| CVE-2025-54055 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup Druco allows Reflected XSS. This issue affects Druco: from n/a through 1.5.2. | Patched by core rule | Y |
| CVE-2025-54046 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QuanticaLabs Cost Calculator allows Stored XSS. This issue affects Cost Calculator: from n/a through 7.4. | Patched by core rule | Y |
| CVE-2025-54044 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in _CreativeMedia_ Elite Video Player allows Reflected XSS. This issue affects Elite Video Player: from n/a through 10.0.5. | Patched by core rule | Y |
| CVE-2025-54032 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebCodingPlace Real Estate Manager Pro allows Reflected XSS. This issue affects Real Estate Manager Pro: from n/a through 12.7.3. | Patched by core rule | Y |
| CVE-2025-54027 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Schiocco Support Board allows Reflected XSS. This issue affects Support Board: from n/a through 3.8.0. | Patched by core rule | Y |
| CVE-2025-53564 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup HTML5 Radio Player - WPBakery Page Builder Addon allows Reflected XSS. This issue affects HTML5 Radio Player - | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | WPBakery Page Builder Addon: from n/a through 2.5. | | |
| CVE-2025-53563 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Youtube Vimeo Video Player and Slider allows Reflected XSS. This issue affects Youtube Vimeo Video Player and Slider: from n/a through 3.8. | Patched by core rule | Y |
| CVE-2025-53562 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player - Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Universal Video Player - Addon for WPBakery Page Builder: from n/a through 3.2.1. | Patched by core rule | Y |
| CVE-2025-53559 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player - Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Universal Video Player - Addon for WPBakery Page Builder: from n/a through 3.2.1. | Patched by core rule | Y |
| CVE-2025-53319 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Raptive Raptive Ads allows Reflected XSS. This issue affects Raptive Ads: from n/a through 3.8.0. | Patched by core rule | Y |
| CVE-2025-53226 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in digitalzoomstudio Comments Capcha Box allows Reflected XSS. This issue affects Comments Capcha Box: from n/a through 1.1. | Patched by core rule | Y |
| CVE-2025-53212 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Revolution Video Player With Bottom Playlist allows Reflected XSS. This issue affects Revolution Video Player With Bottom | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | Playlist: from n/a through 2.9.2. | | |
| CVE-2025-53205 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Radio Player Shoutcast & Icecast allows Reflected XSS. This issue affects Radio Player Shoutcast & Icecast: from n/a through 4.4.7. | Patched by core rule | Y |
| CVE-2025-53201 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NooTheme Jobmonster allows Reflected XSS. This issue affects Jobmonster: from n/a through 4.7.8. | Patched by core rule | Y |
| CVE-2025-53195 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine allows Stored XSS. This issue affects JetEngine: from n/a through 3.7.0. | Patched by core rule | Y |
| CVE-2025-49894 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in rewish WP Emmet allows Stored XSS. This issue affects WP Emmet: from n/a through 0.3.4. | Patched by core rule | Y |
| CVE-2025-49893 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in liseperu Elizaibots allows Stored XSS. This issue affects Elizaibots: from n/a through 1.0.2. | Patched by core rule | Y |
| CVE-2025-49892 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in badasswp Pending Order Bot allows Stored XSS. This issue affects Pending Order Bot: from n/a through 1.0.2. | Patched by core rule | Y |
| CVE-2025-49891 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in riotweb Contact Info Widget allows Stored XSS. This issue affects Contact Info Widget: from n/a through 2.6.2. | Patched by core rule | Y |
| CVE-2025-49890 | CVE-2025 - Improper Neutralization of Input During Web Page | 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 |
|---|---|---|---|---|
| | Generation ('Cross-site Scripting') vulnerability i... | Scripting') vulnerability in Jorge Garcia de Bustos AWStats Script allows Stored XSS. This issue affects AWStats Script: from n/a through 0.3. | | |
| CVE-2025-49889 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in imaprogrammer Custom Comment allows Stored XSS. This issue affects Custom Comment: from n/a through 2.1.6. | Patched by core rule | Y |
| CVE-2025-49436 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in thiudis Custom Menu allows Stored XSS. This issue affects Custom Menu: from n/a through 1.8. | Patched by core rule | Y |
| CVE-2025-49434 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in stijnvanderree Laposta WooCommerce allows Stored XSS. This issue affects Laposta WooCommerce: from n/a through 1.9.1. | Patched by core rule | Y |
| CVE-2025-49428 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dourou Cookie Warning allows Stored XSS. This issue affects Cookie Warning: from n/a through 1.3. | Patched by core rule | Y |
| CVE-2025-49424 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in diego.benna Essential Doo Components for Visual Composer allows DOM-Based XSS. This issue affects Essential Doo Components for Visual Composer: from n/a through 1.9. | Patched by core rule | Y |
| CVE-2025-49422 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aelora iframe Wrapper allows DOM-Based XSS. This issue affects iframe Wrapper: from n/a through 0.1.1. | Patched by core rule | Y |
| CVE-2025-49420 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site | 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 |
|---|---|---|---|---|
| | Scripting') vulnerability i... | Pierre-Henri Lavigne Markup Markdown allows Stored XSS. This issue affects Markup Markdown: from n/a through 3.20.6. | | |
| CVE-2025-49413 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wishloop Terms of Service & Privacy Policy Generator allows Stored XSS. This issue affects Terms of Service & Privacy Policy Generator: from n/a through 1.0. | Patched by core rule | Y |
| CVE-2025-49412 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in numixtech Page Transition allows Stored XSS. This issue affects Page Transition: from n/a through 1.3. | Patched by core rule | Y |
| CVE-2025-49411 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vikas Sharma iFrame Block allows Stored XSS. This issue affects iFrame Block: from n/a through 0.1.1. | Patched by core rule | Y |
| CVE-2025-49410 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Imran Emu TC Testimonials allows Stored XSS. This issue affects TC Testimonials: from n/a through 1.1.1. | Patched by core rule | Y |
| CVE-2025-49409 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brewlabs SensorPress allows Stored XSS. This issue affects SensorPress: from n/a through 1.0. | Patched by core rule | Y |
| CVE-2025-49400 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in osama.esh WP Visitor Statistics (Real Time Traffic) allows Stored XSS. This issue affects WP Visitor Statistics (Real Time Traffic): from n/a through 8.2. | Patched by core rule | Y |
| CVE-2025-49397 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor Alam Colorbox Lightbox allows Stored XSS. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | This issue affects Colorbox Lightbox: from n/a through 1.1.5. | | |
| CVE-2025-49395 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Icons allows Stored XSS. This issue affects Themify Icons: from n/a through 2.0.3. | Patched by core rule | Y |
| CVE-2025-49392 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themifyme Themify Audio Dock allows Stored XSS. This issue affects Themify Audio Dock: from n/a through 2.0.5. | Patched by core rule | Y |
| CVE-2025-49389 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WEN Solutions Notice Bar allows Stored XSS. This issue affects Notice Bar: from n/a through 3.1.3. | Patched by core rule | Y |
| CVE-2025-48297 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in quantumcloud Simple Link Directory allows Reflected XSS. This issue affects Simple Link Directory: from n/a through n/a. | Patched by core rule | Y |
| CVE-2025-48296 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in skygroup UpStore allows Reflected XSS. This issue affects UpStore: from n/a through 1.7.0. | Patched by core rule | Y |
| CVE-2025-48170 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player - Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Universal Video Player - Addon for WPBakery Page Builder: from n/a through 3.2.1. | Patched by core rule | Y |
| CVE-2025-48168 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Apollo - Sticky Full Width HTML5 Audio Player allows | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | Reflected XSS. This issue affects Apollo - Sticky Full Width HTML5 Audio Player: from n/a through 3.4. | | |
| CVE-2025-48163 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup SHOUT - HTML5 Radio Player With Ads - ShoutCast and IceCast Support allows Reflected XSS. This issue affects SHOUT - HTML5 Radio Player With Ads - ShoutCast and IceCast Support: from n/a through 3.5.4. | Patched by core rule | Y |
| CVE-2025-48162 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in quantumcloud Simple Business Directory Pro allows Reflected XSS. This issue affects Simple Business Directory Pro: from n/a through 15.5.1. | Patched by core rule | Y |
| CVE-2025-48159 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Youtube Vimeo Video Player and Slider WP Plugin allows Reflected XSS. This issue affects Youtube Vimeo Video Player and Slider WP Plugin: from n/a through 3.8. | Patched by core rule | Y |
| CVE-2025-48154 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Multimedia Playlist Slider Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Multimedia Playlist Slider Addon for WPBakery Page Builder: from n/a through 2.1. | Patched by core rule | Y |
| CVE-2025-48152 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dimafreund Rentsyst allows Reflected XSS. This issue affects Rentsyst: from n/a through 2.0.100. | Patched by core rule | Y |
| CVE-2025-48151 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Map Locations allows | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | Reflected XSS. This issue affects CM Map Locations: from n/a through 2.1.6. | | |
| CVE-2025-28977 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress WP Pipes allows Reflected XSS. This issue affects WP Pipes: from n/a through 1.4.3. | Patched by core rule | Y |
| CVE-2025-8618 | CVE-2025 - The WPC Smart Quick View for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scr... | The WPC Smart Quick View for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's woosq_btn shortcode in all versions up to, and including, 4.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-9171 | CVE-2025 - A security flaw has been discovered in SolidInvoice up to 2.4.0. The impacted element is an unknown ... | A security flaw has been discovered in SolidInvoice up to 2.4.0. The impacted element is an unknown function of the file /clients of the component Clients Module. Performing manipulation of the argument Name results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-9170 | CVE-2025 - A vulnerability was identified in SolidInvoice up to 2.4.0. The affected element is an unknown funct... | A vulnerability was identified in SolidInvoice up to 2.4.0. The affected element is an unknown function of the file /tax/rates of the component Tax Rates Module. Such manipulation of the argument Name leads to cross site scripting. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-9169 | CVE-2025 - A vulnerability was | A vulnerability was determined in SolidInvoice | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | determined in SolidInvoice up to 2.4.0. Impacted is an unknown function of the f... | up to 2.4.0. Impacted is an unknown function of the file /quotes of the component Quote Module. This manipulation of the argument Name causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. | | |
| CVE-2025-9168 | CVE-2025 - A vulnerability was found in SolidInvoice up to 2.4.0. This issue affects some unknown processing of... | A vulnerability was found in SolidInvoice up to 2.4.0. This issue affects some unknown processing of the file /invoice of the component Invoice Creation Module. The manipulation of the argument Client Name results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-9167 | CVE-2025 - A vulnerability has been found in SolidInvoice up to 2.4.0. This vulnerability affects unknown code ... | A vulnerability has been found in SolidInvoice up to 2.4.0. This vulnerability affects unknown code of the file /invoice/recurring of the component Recurring Invoice Module. The manipulation of the argument client name 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-2025-43744 | CVE-2025 - A stored DOM-based Cross-Site Scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.13... | A stored DOM-based Cross-Site Scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.5, 2025.Q1.0 through 2025.Q1.15, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.19 and 7.4 GA through update 92 exists in the Asset Publisher configuration UI within the Source.js module. This vulnerability allows attackers | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | to inject arbitrary JavaScript via DDM structure field labels which are then inserted into the DOM using innerHTML without proper encoding. | | |
| CVE-2025-43737 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DX... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.8 and 2025.Q1.0 through 2025.Q1.15 allows a remote authenticated user to inject JavaScript code via _com_liferay_journal_web_portlet_JournalPortlet_back URL parameter. | Patched by core rule | Y |
| CVE-2025-43738 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.8, 2025.Q1.0 through 2025.Q1.15, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.19 allows a remote authenticated user to inject JavaScript code via _com_liferay_expando_web_portlet_ExpandoPortlet_displayType parameter. | Patched by core rule | Y |
| CVE-2025-9137 | CVE-2025 - A vulnerability has been found in Scada-LTS 2.7.8.1. This impacts an unknown function of the file sc... | A vulnerability has been found in Scada-LTS 2.7.8.1. This impacts an unknown function of the file scheduled_events.shtm. Such manipulation of the argument alias leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor explains: "[T]he risks of indicated vulnerabilities seem to be minimal as all scenarios likely require admin permissions. Moreover, regardless our team fixes those vulnerabilities - the overall risk change to the user due to malicious admin actions will not be lower. An admin user - by definition - has full control over HTML and JS code that is delivered to users in regular synoptic panels. In other words - due to the design of the system it is not possible to limit the | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | admin user to attack the users." | | |
| CVE-2025-43740 | CVE-2025 - A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.3.120 through 7.4.3.132, and L... | A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.3.120 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.8, 2025.Q1.0 through 2025.Q1.15, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13 and 2024.Q1.9 through 2024.Q1.19 allows an remote authenticated attacker to inject JavaScript through the message boards feature available via the web interface. | Patched by core rule | Y |
| CVE-2025-8783 | CVE-2025 - The Contact Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title... | The Contact Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' parameter in all versions up to, and including, 8.6.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. | Patched by core rule | Y |
| CVE-2025-8567 | CVE-2025 - The Nexter Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple wid... | The Nexter Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 4.5.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8622 | CVE-2025 - The Flexible Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ... | The Flexible Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Flexible Maps shortcode in all versions up to, and including, 1.18.0 due to insufficient input sanitization and output escaping on user supplied attributes. This | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-7496 | CVE-2025 - The WPC Smart Compare for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Script... | The WPC Smart Compare for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via DOM elements in all versions up to, and including, 6.4.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-43731 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.8, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 GA through update 92 allows an remote authenticated user to inject JavaScript in message board threads and categories. | Patched by core rule | Y |
| CVE-2025-43733 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DX... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.7 allows a remote authenticated attacker to inject JavaScript code via the content page's name field. This malicious payload is then reflected and executed within the user's browser when viewing the "document View Usages" page. | Patched by core rule | Y |
| CVE-2025-9107 | CVE-2025 - A vulnerability was determined in Portabilis i-Diario up to 1.5.0. This impacts an unknown function ... | A vulnerability was determined in Portabilis i-Diario up to 1.5.0. This impacts an unknown function of the file /alunos/search_autocomplete. Executing manipulation of the argument q can lead to cross site scripting. The | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | attack may be performed from a remote location. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way. | | |
| CVE-2025-9106 | CVE-2025 - A vulnerability was found in Portabilis i-Diario up to 1.5.0. This affects an unknown function of th... | A vulnerability was found in Portabilis i-Diario up to 1.5.0. This affects an unknown function of the file /planos-de-ensino-por-disciplina/ of the component Informações Adicionais Page. Performing manipulation of the argument Parecer/Conteúdos/Objetivos results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-9105 | CVE-2025 - A vulnerability has been found in Portabilis i-Diario up to 1.5.0. The impacted element is an unknow... | A vulnerability has been found in Portabilis i-Diario up to 1.5.0. The impacted element is an unknown function of the file /planos-de-ensino-por-areas-de-conhecimento/ of the component Informações Adicionais Page. Such manipulation of the argument Parecer/Conteúdos/Objetivos leads to cross site scripting. The attack can be executed 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-2025-9104 | CVE-2025 - A flaw has been found in Portabilis i-Diario up to 1.5.0. The affected element is an unknown functio... | A flaw has been found in Portabilis i-Diario up to 1.5.0. The affected element is an unknown function of the file /planos-de-aulas-por-disciplina/ of the component Informações Adicionais Page. This manipulation of the argument Parecer/Objeto de Conhecimento/Habilidades causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | not respond in any way. | | |
| CVE-2025-9103 | CVE-2025 - A vulnerability was detected in ZenCart 2.1.0. Affected by this vulnerability is an unknown function... | A vulnerability was detected in ZenCart 2.1.0. Affected by this vulnerability is an unknown functionality of the component CKEditor. 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. The real existence of this vulnerability is still doubted at the moment. The vendor declares this as "intended behavior, allowed for authorized administrators". | Patched by core rule | Y |
| CVE-2025-8896 | CVE-2025 - The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugi... | The User Profile Builder – Beautiful User Registration Forms, User Profiles & User Role Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gdpr_communication_preferences[]' parameter in all versions up to, and including, 3.14.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when the GDPR Communication Preferences module is enabled and at least one GDPR Communication Preferences field has been added to the edit profile form. | Patched by core rule | Y |
| CVE-2025-8089 | CVE-2025 - The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'addit... | The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'additional' parameter in version less than, or equal to, 2025.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-6221 | CVE-2025 - The Embed Bokun plugin for WordPress is vulnerable to Stored Cross-Site | The Embed Bokun plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘align’ parameter in | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | Scripting via the ‘align’ pa... | all versions up to, and including, 0.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-49898 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Xolluteon Dropshix allows DOM-Based XSS.This issue affects Dropshix: from n/a through 4.0.14. | Patched by core rule | Y |
| CVE-2025-8080 | CVE-2025 - The Alobaidi Captcha plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugi... | The Alobaidi Captcha plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 1.0.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. | Patched by core rule | Y |
| CVE-2025-5844 | CVE-2025 - The Radius Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘subHead... | The Radius Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘subHeadingTagName’ parameter in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8604 | CVE-2025 - The WP Table Builder – WordPress Table Plugin plugin for WordPress is vulnerable to Stored Cross-Sit... | The WP Table Builder – WordPress Table Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wptb shortcode in all versions up to, and including, 2.0.12 due to | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-8451 | CVE-2025 - The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is v... | The Essential Addons for Elementor – Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via the 'data-gallery-items' parameter in all versions up to, and including, 6.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8867 | CVE-2025 - The Graphina - Elementor Charts and Graphs plugin for WordPress is vulnerable to Stored Cross-Site S... | The Graphina - Elementor Charts and Graphs plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple chart widget parameters in version 3.1.3 and below. This is due to insufficient input sanitization and output escaping on user supplied attributes such as chart categories, titles, and tooltip settings. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8975 | CVE-2025 - A vulnerability was identified in givanz Vvveb up to 1.0.5. This affects an unknown part of the file... | A vulnerability was identified in givanz Vvveb up to 1.0.5. This affects an unknown part of the file admin/template/content/edit.tpl. The manipulation of the argument slug 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 1.0.6 is able to address this issue. The patch is named 84c11d69df8452dc378feecd17e2a62ac10dac66. It is | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | recommended to upgrade the affected component. | | |
| CVE-2025-55714 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetElements For Elementor allows Stored XSS. This issue affects JetElements For Elementor: from n/a through 2.7.9. | Patched by core rule | Y |
| CVE-2025-55713 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeThemes Blocksy allows Stored XSS. This issue affects Blocksy: from n/a through 2.1.6. | Patched by core rule | Y |
| CVE-2025-55711 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Table Builder WP Table Builder allows Stored XSS. This issue affects WP Table Builder: from n/a through 2.0.12. | Patched by core rule | Y |
| CVE-2025-55709 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visual Composer Visual Composer Website Builder allows Stored XSS. This issue affects Visual Composer Website Builder: from n/a through n/a. | Patched by core rule | Y |
| CVE-2025-54749 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetProductGallery allows Stored XSS. This issue affects JetProductGallery: from n/a through 2.2.0.2. | Patched by core rule | Y |
| CVE-2025-54747 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpbakery Templatera allows DOM-Based XSS. This issue affects Templatera: from n/a through 2.3.0. | Patched by core rule | Y |
| CVE-2025-54746 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cartpauj Shortcode Redirect allows Stored XSS. This issue affects Shortcode Redirect: from n/a through 1.0.02. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-54740 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Nelson Print My Blog allows Stored XSS. This issue affects Print My Blog: from n/a through 3.27.9. | Patched by core rule | Y |
| CVE-2025-54729 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webba Appointment Booking Webba Booking allows Stored XSS. This issue affects Webba Booking: from n/a through 6.0.5. | Patched by core rule | Y |
| CVE-2025-54727 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CreativeMindsSolutions CM On Demand Search And Replace allows Stored XSS. This issue affects CM On Demand Search And Replace: from n/a through 1.5.2. | Patched by core rule | Y |
| CVE-2025-54708 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins B Blocks allows DOM-Based XSS. This issue affects B Blocks: from n/a through 2.0.5. | Patched by core rule | Y |
| CVE-2025-54054 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AA Web Servant 12 Step Meeting List allows Stored XSS. This issue affects 12 Step Meeting List: from n/a through 3.18.3. | Patched by core rule | Y |
| CVE-2025-53582 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WordLift WordLift allows Stored XSS. This issue affects WordLift: from n/a through 3.54.5. | Patched by core rule | Y |
| CVE-2025-53581 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in artiosmedia RSS Feed Pro allows Stored XSS. This issue affects RSS Feed Pro: from n/a through 1.1.8. | Patched by core rule | Y |
| CVE-2025-53575 | CVE-2025 - Improper Neutralization of Input | Improper Neutralization of Input During Web Page | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | During Web Page Generation ('Cross-site Scripting') vulnerability i... | Generation ('Cross-site Scripting') vulnerability in primersoftware Primer MyData for Woocommerce allows Reflected XSS. This issue affects Primer MyData for Woocommerce: from n/a through 4.2.5. | | |
| CVE-2025-53342 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GoodLayers Modernize allows Stored XSS. This issue affects Modernize: from n/a through 3.4.0. | Patched by core rule | Y |
| CVE-2025-53330 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WpEstate WP Rentals allows Stored XSS. This issue affects WP Rentals: from n/a through 3.13.1. | Patched by core rule | Y |
| CVE-2025-52771 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bcupham Video Expander allows Stored XSS. This issue affects Video Expander: from n/a through 1.0. | Patched by core rule | Y |
| CVE-2024-37945 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPBits WPBITS Addons For Elementor Page Builder allows Stored XSS.This issue affects WPBITS Addons For Elementor Page Builder: from n/a through 1.5. | Patched by core rule | Y |
| CVE-2025-54706 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noor Alam Magical Posts Display allows DOM-Based XSS. This issue affects Magical Posts Display: from n/a through 1.2.52. | Patched by core rule | Y |
| CVE-2025-54704 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hashthemes Easy Elementor Addons allows DOM-Based XSS. This issue affects Easy Elementor Addons: from n/a through 2.2.6. | Patched by core rule | Y |
| CVE-2025-54699 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site | 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 |
|---|---|---|---|---|
| | Scripting') vulnerability i... | masteriyo Masteriyo - LMS allows Stored XSS. This issue affects Masteriyo - LMS: from n/a through 1.18.3. | | |
| CVE-2025-54696 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFunnels WPFunnels allows Stored XSS. This issue affects WPFunnels: from n/a through 3.5.26. | Patched by core rule | Y |
| CVE-2025-54688 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine allows Stored XSS. This issue affects JetEngine: from n/a through 3.7.1.2. | Patched by core rule | Y |
| CVE-2025-54687 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetTabs allows DOM-Based XSS. This issue affects JetTabs: from n/a through 2.2.9.1. | Patched by core rule | Y |
| CVE-2025-54684 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CRM Perks Integration for Contact Form 7 and Constant Contact allows Stored XSS. This issue affects Integration for Contact Form 7 and Constant Contact: from n/a through 1.1.7. | Patched by core rule | Y |
| CVE-2025-54683 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Astoundify WP Modal Popup with Cookie Integration allows Reflected XSS. This issue affects WP Modal Popup with Cookie Integration: from n/a through 2.4. | Patched by core rule | Y |
| CVE-2025-54680 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sparkle Themes Blogger Buzz allows Stored XSS. This issue affects Blogger Buzz: from n/a through 1.2.6. | Patched by core rule | Y |
| CVE-2025-54676 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in vcita Online Booking & Scheduling Calendar for | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | WordPress by vcita allows Stored XSS. This issue affects Online Booking & Scheduling Calendar for WordPress by vcita: from n/a through 4.5.3. | | |
| CVE-2025-54668 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saad Iqbal myCred allows Stored XSS. This issue affects myCred: from n/a through 2.9.4.3. | Patched by core rule | Y |
| CVE-2025-52788 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Russell Jamieson CaptionPix allows Reflected XSS. This issue affects CaptionPix: from n/a through 1.8. | Patched by core rule | Y |
| CVE-2025-52730 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in themefunction WordPress Event Manager, Event Calendar and Booking Plugin allows Stored XSS. This issue affects WordPress Event Manager, Event Calendar and Booking Plugin: from n/a through 4.0.24. | Patched by core rule | Y |
| CVE-2025-50040 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in moshensky CF7 Spreadsheets allows Stored XSS. This issue affects CF7 Spreadsheets: from n/a through 2.3.2. | Patched by core rule | Y |
| CVE-2025-49437 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in worstguy WP LOL Rotation allows Stored XSS. This issue affects WP LOL Rotation: from n/a through 1.0. | Patched by core rule | Y |
| CVE-2025-49433 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThanhD Supermalink allows DOM-Based XSS. This issue affects Supermalink: from n/a through 1.1. | Patched by core rule | Y |
| CVE-2025-49065 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BestiaDurmiente Visit | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | i... | Counter allows Stored XSS. This issue affects Visit Counter: from n/a through 1.0. | | |
| CVE-2025-49064 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webilop User Language Switch allows Reflected XSS. This issue affects User Language Switch: from n/a through 1.6.10. | Patched by core rule | Y |
| CVE-2025-49063 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in i3geek BaiduXZH Submit(百度熊掌号) allows Reflected XSS. This issue affects BaiduXZH Submit(百度熊掌号): from n/a through 1.4.6. | Patched by core rule | Y |
| CVE-2025-49062 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cornfeed WP-jScrollPane allows Reflected XSS. This issue affects WP-jScrollPane: from n/a through 2.0.3. | Patched by core rule | Y |
| CVE-2025-49061 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in perteus Porn Videos Embed allows Stored XSS. This issue affects Porn Videos Embed: from n/a through 0.9.1. | Patched by core rule | Y |
| CVE-2025-49058 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sound Strategies SoundSt SEO Search allows Reflected XSS. This issue affects SoundSt SEO Search: from n/a through 1.2.3. | Patched by core rule | Y |
| CVE-2025-49057 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ko Min WP Voting allows Reflected XSS. This issue affects WP Voting: from n/a through 1.8. | Patched by core rule | Y |
| CVE-2025-49056 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shen2 多说社会化评论框 allows Reflected XSS. This issue affects 多说社会化评 | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | 论框: from n/a through 1.2. | | |
| CVE-2025-49054 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mrdenny Time Sheets allows Reflected XSS. This issue affects Time Sheets: from n/a through 2.1.3. | Patched by core rule | Y |
| CVE-2025-49053 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kadesthemes WP Airdrop Manager allows Stored XSS. This issue affects WP Airdrop Manager: from n/a through 1.0.5. | Patched by core rule | Y |
| CVE-2025-49051 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in biscia7 Hide Text Shortcode allows Stored XSS. This issue affects Hide Text Shortcode: from n/a through 1.1. | Patched by core rule | Y |
| CVE-2025-49048 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in inspectlet Inspectlet – User Session Recording and Heatmaps allows Stored XSS. This issue affects Inspectlet – User Session Recording and Heatmaps: from n/a through 2.0. | Patched by core rule | Y |
| CVE-2025-49047 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in keeross DigitalOcean Spaces Sync allows Stored XSS. This issue affects DigitalOcean Spaces Sync: from n/a through 2.2.1. | Patched by core rule | Y |
| CVE-2025-49038 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Soflyy WP Dynamic Links allows Reflected XSS. This issue affects WP Dynamic Links: from n/a through 1.0.1. | Patched by core rule | Y |
| CVE-2025-49037 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Federico Rota Authentication and xmlrpc log writer allows Reflected | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | XSS. This issue affects Authentication and xmlrpc log writer: from n/a through 1.2.2. | | |
| CVE-2025-47689 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in johnh10 Video Blogster Lite allows Reflected XSS. This issue affects Video Blogster Lite: from n/a through 1.2. | Patched by core rule | Y |
| CVE-2025-47610 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wetail WooCommerce Fortnox Integration allows Stored XSS. This issue affects WooCommerce Fortnox Integration: from n/a through 4.5.6. | Patched by core rule | Y |
| CVE-2025-31007 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alvind Billplz Addon for Contact Form 7 allows Reflected XSS. This issue affects Billplz Addon for Contact Form 7: from n/a through 1.2.0. | Patched by core rule | Y |
| CVE-2025-30626 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Multimedia Playlist Slider Addon for WPBakery Page Builder allows Reflected XSS. This issue affects Multimedia Playlist Slider Addon for WPBakery Page Builder: from n/a through 2.1. | Patched by core rule | Y |
| CVE-2025-29014 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZoomIt FoodMenu allows Reflected XSS. This issue affects FoodMenu: from n/a through 1.20. | Patched by core rule | Y |
| CVE-2025-28999 | CVE-2025 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability i... | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZoomIt WooCommerce Shop Page Builder allows Reflected XSS. This issue affects WooCommerce Shop Page Builder: from n/a through 2.27.7. | Patched by core rule | Y |
| CVE-2025-28975 | CVE-2025 - Improper Neutralization of Input | Improper Neutralization of Input During Web Page | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | During Web Page Generation ('Cross-site Scripting') vulnerability i... | Generation ('Cross-site Scripting') vulnerability in redqteam Alike - WordPress Custom Post Comparison allows Reflected XSS. This issue affects Alike - WordPress Custom Post Comparison: from n/a through 3.0.1. | | |
| CVE-2025-43982 | CVE-2025 - Shenzhen Tuoshi NR500-EA RG500UEAABxCOMSLICv 3.4.2731.16.43 devices enable the SSH service by default... | Shenzhen Tuoshi NR500-EA RG500UEAABxCOMSLICv3.4. 2731.16.43 devices enable the SSH service by default. There is a hidden hard-coded root account that cannot be disabled in the GUI. | Patched by core rule | Y |
| CVE-2025-45313 | CVE-2025 - A cross-site scripting (XSS) vulnerability in the /tasks endpoint of hortusfox-web v4.4 allows attac... | A cross-site scripting (XSS) vulnerability in the /tasks endpoint of hortusfox-web v4.4 allows attackers to execute arbitrary JavaScript in the context of a user's browser via a crafted payload injected into the title parameter. | Patched by core rule | Y |
| CVE-2025-8920 | CVE-2025 - A vulnerability was identified in Portabilis i-Diario 1.6. Affected by this vulnerability is an unkn... | A vulnerability was identified in Portabilis i-Diario 1.6. Affected by this vulnerability is an unknown functionality of the file /dicionario-de-termos-bncc of the component Dicionário de Termos BNCC Page. The manipulation of the argument Planos de ensino 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-2025-8919 | CVE-2025 - A vulnerability was determined in Portabilis i-Diario up to 1.6. Affected is an unknown function of ... | A vulnerability was determined in Portabilis i-Diario up to 1.6. Affected is an unknown function of the file /objetivos-de-aprendizagem-e-habilidades of the component History Page. The manipulation of the argument código/objetivo habilidade 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-2025-45316 | CVE-2025 - A cross-site scripting (XSS) vulnerability in the | A cross-site scripting (XSS) vulnerability in the TextBlockModule.php | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | TextBlockModule.php component of hortusfox-web v4.... | component of hortusfox-web v4.4 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the name parameter. | | |
| CVE-2025-45315 | CVE-2025 - A cross-site scripting (XSS) vulnerability in the /controller/admin.php endpoint of hortusfox-web v4... | A cross-site scripting (XSS) vulnerability in the /controller/admin.php endpoint of hortusfox-web v4.4 allows attackers to execute arbitrary JavaScript in the context of a user's browser via a crafted payload injected into the email parameter. | Patched by core rule | Y |
| CVE-2025-45314 | CVE-2025 - A cross-site scripting (XSS) vulnerability in the /Calendar endpoint of hortusfox-web v4.4 allows at... | A cross-site scripting (XSS) vulnerability in the /Calendar endpoint of hortusfox-web v4.4 allows attackers to execute arbitrary JavaScript in the context of a user's browser via a crafted payload injected into the add function. | Patched by core rule | Y |
| CVE-2025-8918 | CVE-2025 - A vulnerability was found in Portabilis i-Educar up to 2.10. This issue affects some unknown process... | A vulnerability was found in Portabilis i-Educar up to 2.10. This issue affects some unknown processing of the file /intranet/educar_instituicao_cad.php of the component Editar Page. The manipulation of the argument neighborhood name 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-2025-51691 | CVE-2025 - Cross-Site Scripting (XSS) vulnerability found in MarkTwo commit e3a1d3f90cce4ea9c26efcbbf3a1cbfb9dc... | Cross-Site Scripting (XSS) vulnerability found in MarkTwo commit e3a1d3f90cce4ea9c26efcbbf3a1cbfb9dcdb298 (May 2025) allows a remote attacker to execute arbitrary code via a crafted script input to the editor interface. The application does not properly sanitize user-supplied Markdown before rendering it. Successful exploitation could lead to session hijacking, credential theft, or arbitrary client-side code execution in the context of the victim's browser. | Patched by core rule | Y |
| CVE-2025-43734 | CVE-2025 - A reflected | A reflected cross-site | Patched by core | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, ... | scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.10, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 GA through update 92 allows a remote authenticated attacker to inject JavaScript code in the “first display label” field in the configuration of a custom sort widget. This malicious payload is then reflected and executed by clay button taglib when refreshing the page. | rule | |
| CVE-2025-43735 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the google_gadget. | Patched by core rule | Y |
| CVE-2025-8874 | CVE-2025 - The Master Addons – Elementor Addons with White Label, Free Widgets, Hover Effects, Conditions, & An... | The Master Addons – Elementor Addons with White Label, Free Widgets, Hover Effects, Conditions, & Animations plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widgets in all versions up to, and including, 2.0.8.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8314 | CVE-2025 - The Software Issue Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the... | The Software Issue Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘noaccess_msg parameter in all versions up to, and including, 5.0.1 due to insufficient input sanitization and output escaping. This | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-8788 | CVE-2025 - A vulnerability was found in Portabilis i-Diario up to 1.5.0 and classified as problematic. Affected... | A vulnerability was found in Portabilis i-Diario up to 1.5.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /planos-de-aula-por-areas-de-conhecimento/ of the component Informações adicionais. The manipulation of the argument Parecer/Conteúdos/Objetivos 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. | Patched by core rule | Y |
| CVE-2025-8787 | CVE-2025 - A vulnerability has been found in Portabilis i-Diario up to 1.5.0 and classified as problematic. Aff... | A vulnerability has been found in Portabilis i-Diario up to 1.5.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /registros-de-conteudos-por-disciplina/ of the component Registro das atividades. The manipulation of the argument Registro de atividades/Conteúdos 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-2025-8786 | CVE-2025 - A vulnerability, which was classified as problematic, was found in Portabilis i-Diario up to 1.5.0. ... | A vulnerability, which was classified as problematic, was found in Portabilis i-Diario up to 1.5.0. Affected is an unknown function of the file /registros-de-conteudos-por-areas-de-conhecimento/ of the component Registro das atividades. The manipulation of the argument Registro de atividades/Conteúdos 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 | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | about this disclosure but did not respond in any way. | | |
| CVE-2025-8785 | CVE-2025 - A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar up to 2.... | A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar up to 2.9. This issue affects some unknown processing of the file /intranet/educar_usuario_lst.php. The manipulation of the argument nm_pessoa/matricula/matricula_interna 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-2025-8784 | CVE-2025 - A vulnerability classified as problematic was found in Portabilis i-Educar up to 2.9. This vulnerabi... | A vulnerability classified as problematic was found in Portabilis i-Educar up to 2.9. This vulnerability affects unknown code of the file /intranet/funcionario_vinculo_cad.php of the component Cadastrar Vínculo Page. The manipulation of the argument nome 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-2025-8743 | CVE-2025 - A vulnerability classified as problematic has been found in Scada-LTS up to 2.7.8.1. This affects an... | A vulnerability classified as problematic has been found in Scada-LTS up to 2.7.8.1. This affects an unknown part of the file /data_source_edit.shtm of the component Virtual Data Source Property Handler. The manipulation of the argument Name 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-2025-4576 | CVE-2025 - A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.133, ... | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.133, and Liferay DXP 2025.Q1.0 through 2025.Q1.4 ,2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15, 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the modules/apps/blogs/blogs-web/src/main/resources/META-INF/resources/blogs/entry_cover_image_caption.jsp | | |
| CVE-2020-9322 | CVE-2025 - The /users endpoint in Statamic Core before 2.11.8 allows XSS to add an administrator user. This can... | The /users endpoint in Statamic Core before 2.11.8 allows XSS to add an administrator user. This can be exploited via CSRF. Stored XSS can occur via a JavaScript payload in a username during account registration. Reflected XSS can occur via the /users PATH_INFO. | Patched by core rule | Y |
| CVE-2025-51629 | CVE-2025 - A cross-site scripting (XSS) vulnerability in the PdfViewer component of Agenzia Impresa Eccobook 2.... | A cross-site scripting (XSS) vulnerability in the PdfViewer component of Agenzia Impresa Eccobook 2.81.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Temp parameter. | Patched by core rule | Y |
| CVE-2023-41529 | CVE-2025 - Hospital Management System v4 was discovered to contain multiple cross-site scripting (XSS) vulnerab... | Hospital Management System v4 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities in func2.php via the fname and lname parameters. | Patched by core rule | Y |
| CVE-2023-41519 | CVE-2025 - Student Attendance Management System v1 was discovered to contain a cross-site scripting (XSS) vulne... | Student Attendance Management System v1 was discovered to contain a cross-site scripting (XSS) vulnerability via the sessionName parameter at createSessionTerm.php. | Patched by core rule | Y |
| CVE-2025-55134 | CVE-2025 - In Agora Foundation Agora fall23-Alpha1 before b087490, there is XSS via tag in client/agora/public/... | In Agora Foundation Agora fall23-Alpha1 before b087490, there is XSS via tag in client/agora/public/js/editorManager.js. | Patched by core rule | Y |
| CVE-2025-55133 | CVE-2025 - In Agora Foundation Agora fall23-Alpha1 before b087490, there is XSS via topicName in client/agora/p... | In Agora Foundation Agora fall23-Alpha1 before b087490, there is XSS via topicName in client/agora/public/js/editorManager.js. | Patched by core rule | Y |
| CVE-2024-52680 | CVE-2025 - EyouCMS 1.6.7 is vulnerable to Cross Site Scripting (XSS) in /login.php?m=admin&c=System&a=web&lang=... | EyouCMS 1.6.7 is vulnerable to Cross Site Scripting (XSS) in /login.php?m=admin&c=System&a=web&lang=cn. | Patched by core rule | Y |
| CVE-2025-50740 | CVE-2025 - AutoConnect | AutoConnect 1.4.2, an | Patched by core | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | 1.4.2, an Arduino library, is vulnerable to a cross site scripting (xss) vulnerability. ... | Arduino library, is vulnerable to a cross site scripting (xss) vulnerability. The AutoConnect web interface /_ac/config allows HTML/JS code to be executed via a crafted network SSID. | rule | |
| CVE-2025-7727 | CVE-2025 - The Gutenverse plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's An... | The Gutenverse plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Animated Text and Fun Fact blocks in all versions up to, and including, 3.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8100 | CVE-2025 - The Element Pack Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-S... | The Element Pack Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'marker_content' parameter in versions up to, and including, 8.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-7498 | CVE-2025 - The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting... | The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown Widget in all versions up to, and including, 2.7.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-6256 | CVE-2025 - The Flex Guten plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'thumbnailH... | The Flex Guten plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'thumbnailHoverEffect' parameter in all versions up to, and including, 1.2.5 due | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-51541 | CVE-2025 - A stored cross-site scripting (XSS) vulnerability exists in the Shopware 6 installation interface at... | A stored cross-site scripting (XSS) vulnerability exists in the Shopware 6 installation interface at /recovery/install/database-configuration/. The c_database_schema field fails to properly sanitize user-supplied input before rendering it in the browser, allowing an attacker to inject malicious JavaScript. This vulnerability can be exploited via a Cross-Site Request Forgery (CSRF) attack due to the absence of CSRF protections on the POST request. An unauthenticated remote attacker can craft a malicious web page that, when visited by a victim, stores the payload persistently in the installation configuration. As a result, the payload executes whenever any user subsequently accesses the vulnerable installation page, leading to persistent client-side code execution. | Patched by core rule | Y |
| CVE-2025-50592 | CVE-2025 - Cross site scripting vulnerability in seacms before 13.2 via the vid parameter to Upload/js/player/d... | Cross site scripting vulnerability in seacms before 13.2 via the vid parameter to Upload/js/player/dmplayer/player. | Patched by core rule | Y |
| CVE-2025-51857 | CVE-2025 - The reconcile method in the AttachmentReconciler class of the Halo system v.2.20.18LTS and before is... | The reconcile method in the AttachmentReconciler class of the Halo system v.2.20.18LTS and before is vulnerable to XSS attacks. | Patched by core rule | Y |
| CVE-2025-8295 | CVE-2025 - The Employee Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘no... | The Employee Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘noaccess_msg’ parameter in all versions up to, and including, 4.5.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-8294 | CVE-2025 - The Download Counter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name... | The Download Counter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8315 | CVE-2025 - The WP Easy Contact plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'noacc... | The WP Easy Contact plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'noaccess_msg' parameter in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8313 | CVE-2025 - The Campus Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'noac... | The Campus Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'noaccess_msg' parameter in all versions up to, and including, 1.9.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8540 | CVE-2025 - A vulnerability was found in Portabilis i-Educar 2.10. It has been classified as problematic. This a... | A vulnerability was found in Portabilis i-Educar 2.10. It has been classified as problematic. This affects an unknown part of the file /intranet/public_municipio_cad.php. The manipulation of the argument nome leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | and may be used. The vendor was contacted early about this disclosure but did not respond in any way. | | |
| CVE-2025-8539 | CVE-2025 - A vulnerability was found in Portabilis i-Educar 2.10 and classified as problematic. Affected by thi... | A vulnerability was found in Portabilis i-Educar 2.10 and classified as problematic. Affected by this issue is some unknown functionality of the file /intranet/public_distrito_cad.php. The manipulation of the argument nome 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. | Patched by core rule | Y |
| CVE-2025-8538 | CVE-2025 - A vulnerability has been found in Portabilis i-Educar 2.10 and classified as problematic. Affected b... | A vulnerability has been found in Portabilis i-Educar 2.10 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /usuarios/tipos/novo. The manipulation of the argument name/description 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-2025-8535 | CVE-2025 - A vulnerability, which was classified as problematic, has been found in cronoh NanoVault up to 1.2.1... | A vulnerability, which was classified as problematic, has been found in cronoh NanoVault up to 1.2.1. This issue affects the function executeJavaScript of the file /main.js of the component xrb URL Handler. The manipulation 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-2025-4604 | CVE-2025 - The vulnerable code can bypass the Captcha check in Liferay Portal 7.4.3.80 through 7.4.3.132, and L... | The vulnerable code can bypass the Captcha check in Liferay Portal 7.4.3.80 through 7.4.3.132, and Liferay DXP 2024.Q1.1 through 2024.Q1.19, 2024.Q2.0 through 2024.Q2.13, 2024.Q3.0 through 2024.Q3.13, 2024.Q4.0 through | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | 2024.Q4.7, 2025.Q1.0 through 2025.Q1.15 and 7.4 update 80 through update 92 and then attackers can run scripts in the Gogo shell | | |
| CVE-2025-4599 | CVE-2025 - The fragment preview functionality in Liferay Portal 7.4.3.61 through 7.4.3.132, and Liferay DXP 202... | The fragment preview functionality in Liferay Portal 7.4.3.61 through 7.4.3.132, and Liferay DXP 2024.Q4.1 through 2024.Q4.5, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.13 and 7.4 update 61 through update 92 was found to be vulnerable to postMessage-based XSS because it allows a remote non-authenticated attacker to inject JavaScript into the fragment portlet URL. | Patched by core rule | Y |
| CVE-2025-50754 | CVE-2025 - Unisite CMS version 5.0 contains a stored Cross-Site Scripting (XSS) vulnerability in the "Report" f... | Unisite CMS version 5.0 contains a stored Cross-Site Scripting (XSS) vulnerability in the "Report" functionality. A malicious script submitted by an attacker is rendered in the admin panel when viewed by an administrator. This allows attackers to hijack the admin session and, by leveraging the template editor, upload and execute a PHP web shell on the server, leading to full remote code execution. | Patched by core rule | Y |
| CVE-2025-8511 | CVE-2025 - A vulnerability classified as problematic was found in Portabilis i-Diario 1.5.0. This vulnerability... | A vulnerability classified as problematic was found in Portabilis i-Diario 1.5.0. This vulnerability affects unknown code of the file /diario-de-observacoes/ of the component Observações. The manipulation of the argument Descrição 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-2025-8510 | CVE-2025 - A vulnerability classified as problematic has been found in Portabilis i-Educar 2.10. This affects t... | A vulnerability classified as problematic has been found in Portabilis i-Educar 2.10. This affects the function Gerar of the file ieducar/intranet/educar_matricula_lst.php. The manipulation of the argument ref_cod_aluno leads to cross site scripting. | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 82c288b9a4abb084bdfa1c0c4ef777ed45f98b46. It is recommended to apply a patch to fix this issue. The vendor initially closed the original advisory without requesting a CVE. | | |
| CVE-2025-8509 | CVE-2025 - A vulnerability was found in Portabilis i-Educar 2.9. It has been rated as problematic. Affected by ... | A vulnerability was found in Portabilis i-Educar 2.9. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /intranet/educar_servidor_cad.php. The manipulation of the argument matricula 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. | Patched by core rule | Y |
| CVE-2025-8508 | CVE-2025 - A vulnerability was found in Portabilis i-Educar 2.9. It has been declared as problematic. Affected ... | A vulnerability was found in Portabilis i-Educar 2.9. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /intranet/educar_avaliacao_desempenho_cad.php. The manipulation of the argument titulo_avaliacao/descricao 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-2025-8507 | CVE-2025 - A vulnerability was found in Portabilis i-Educar 2.9. It has been classified as problematic. Affecte... | A vulnerability was found in Portabilis i-Educar 2.9. It has been classified as problematic. Affected is an unknown function of the file /intranet/educar_funcao_lst.php. The manipulation of the argument nm_funcao/abreviatura 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 |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-8506 | CVE-2025 - A vulnerability was found in 495300897 wx-shop up to de1b66331368695779cfc6e4d11a64caddf8716e and cl... | A vulnerability was found in 495300897 wx-shop up to de1b66331368695779cfc6e4d11a64caddf8716e and classified as problematic. This issue affects some unknown processing of the file /user/editUI. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. | Patched by core rule | Y |
| CVE-2025-8501 | CVE-2025 - A vulnerability classified as problematic has been found in code-projects Human Resource Integrated ... | A vulnerability classified as problematic has been found in code-projects Human Resource Integrated System 1.0. Affected is an unknown function of the file /insert-and-view/action.php. The manipulation of the argument 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. | Patched by core rule | Y |
| CVE-2025-7500 | CVE-2025 - The Ocean Social Sharing plugin for WordPress is vulnerable to Stored Cross-Site Scripting via socia... | The Ocean Social Sharing plugin for WordPress is vulnerable to Stored Cross-Site Scripting via social icon titles in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-6832 | CVE-2025 - The All in One Time Clock Lite – Tracking Employee Time Has Never Been Easier plugin for WordPress i... | The All in One Time Clock Lite – Tracking Employee Time Has Never Been Easier plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'nonce' parameter in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | can successfully trick a user into performing an action such as clicking on a link. | | |
| CVE-2025-6626 | CVE-2025 - The ShortPixel Adaptive Images – WebP, AVIF, CDN, Image Optimization plugin for WordPress is vulnera... | The ShortPixel Adaptive Images – WebP, AVIF, CDN, Image Optimization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the API URL Setting in all versions up to, and including, 3.10.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. | Patched by core rule | Y |
| CVE-2025-8146 | CVE-2025 - The Qi Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via th... | The Qi Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's TypeOut Text widget in all versions up to, and including, 1.9.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-50869 | CVE-2025 - A stored Cross-Site Scripting (XSS) vulnerability exists in the qureydetails.php page of Institute-o... | A stored Cross-Site Scripting (XSS) vulnerability exists in the qureydetails.php page of Institute-of-Current-Students 1.0, where the input fields for Query and Answer do not properly sanitize user input. Authenticated users can inject arbitrary JavaScript code. | Patched by core rule | Y |
| CVE-2025-51504 | CVE-2025 - Microweber CMS 2.0 is vulnerable to Cross Site Scripting (XSS)in the /projects/profile, homepage end... | Microweber CMS 2.0 is vulnerable to Cross Site Scripting (XSS)in the /projects/profile, homepage endpoint via the last name field. | Patched by core rule | Y |
| CVE-2025-51502 | CVE-2025 - Reflected Cross-Site Scripting (XSS) in Microweber CMS 2.0 via the layout parameter on the /admin/pa... | Reflected Cross-Site Scripting (XSS) in Microweber CMS 2.0 via the layout parameter on the /admin/page/create page allows arbitrary JavaScript execution in the context of | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | authenticated admin users. | | |
| CVE-2025-51501 | CVE-2025 - Reflected Cross-Site Scripting (XSS) in the id parameter of the live_edit.module_settings API endpoi... | Reflected Cross-Site Scripting (XSS) in the id parameter of the live_edit.module_settings API endpoint in Microweber CMS2.0 allows execution of arbitrary JavaScript. | Patched by core rule | Y |
| CVE-2025-6228 | CVE-2025 - The Sina Extension for Elementor (Header Builder, Footer Builter, Theme Builder, Slider, Gallery, Fo... | The Sina Extension for Elementor (Header Builder, Footer Builter, Theme Builder, Slider, Gallery, Form, Modal, Data Table Free Elementor Widgets & Elementor Templates) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `Sina Posts`, `Sina Blog Post` and `Sina Table` widgets in all versions up to, and including, 3.7.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-4684 | CVE-2025 - The BlockSpare: Gutenberg Blocks & Patterns for Blogs, Magazines, Business Sites – Post Grids, Slide... | The BlockSpare: Gutenberg Blocks & Patterns for Blogs, Magazines, Business Sites – Post Grids, Sliders, Carousels, Counters, Page Builder & Starter Site Imports, No Coding Needed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the HTML attributes of Image Carousel and Image Slider widgets in all versions up to, and including, 3.2.13.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-7646 | CVE-2025 - The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerc... | The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom script parameter in all versions up to, and including, 6.3.10 | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | even when the user does not have the unfiltered_html capability. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-7845 | CVE-2025 - The Stratum – Elementor Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting vi... | The Stratum – Elementor Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Advanced Google Maps and Image Hotspot widgets in all versions up to, and including, 1.6.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-7725 | CVE-2025 - The Photos, Files, YouTube, Twitter, Instagram, TikTok, Ecommerce Contest Gallery – Upload, Vote, Se... | The Photos, Files, YouTube, Twitter, Instagram, TikTok, Ecommerce Contest Gallery – Upload, Vote, Sell via PayPal or Stripe, Social Share Buttons, OpenAI plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the comment feature in all versions up to, and including, 26.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-51503 | CVE-2025 - A Stored Cross-Site Scripting (XSS) vulnerability in Microweber CMS 2.0 allows attackers to inject m... | A Stored Cross-Site Scripting (XSS) vulnerability in Microweber CMS 2.0 allows attackers to inject malicious scripts into user profile fields, leading to arbitrary JavaScript execution in admin browsers. | Patched by core rule | Y |
| CVE-2025-50866 | CVE-2025 - CloudClassroom-PHP-Project 1.0 contains a reflected Cross-site Scripting (XSS) vulnerability in the ... | CloudClassroom-PHP-Project 1.0 contains a reflected Cross-site Scripting (XSS) vulnerability in the email parameter of the postquerypublic endpoint. Improper sanitization allows an attacker to inject arbitrary JavaScript code | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | that executes in the context of the user s browser, potentially leading to session hijacking or phishing attacks. | | |
| CVE-2025-52203 | CVE-2025 - A stored cross-site scripting (XSS) vulnerability exists in DevaslanPHP project-management v1.2.4. T... | A stored cross-site scripting (XSS) vulnerability exists in DevaslanPHP project-management v1.2.4. The vulnerability resides in the Ticket Name field, which fails to properly sanitize user-supplied input. An authenticated attacker can inject malicious JavaScript payloads into this field, which are subsequently stored in the database. When a legitimate user logs in and is redirected to the Dashboard panel "automatically upon authentication the malicious script executes in the user's browser context. | Patched by core rule | Y |
| CVE-2025-50848 | CVE-2025 - A file upload vulnerability was discovered in CS Cart 4.18.3, allows attackers to execute arbitrary ... | A file upload vulnerability was discovered in CS Cart 4.18.3, allows attackers to execute arbitrary code. CS Cart 4.18.3 allows unrestricted upload of HTML files, which are rendered directly in the browser when accessed. This allows an attacker to upload a crafted HTML file containing malicious content, such as a fake login form for credential harvesting or scripts for Cross-Site Scripting (XSS) attacks. Since the content is served from a trusted domain, it significantly increases the likelihood of successful phishing or script execution against other users. | Patched by core rule | Y |
| CVE-2025-50270 | CVE-2025 - A stored Cross Site Scripting (xss) vulnerability in the "content management" feature in AnQiCMS v.3... | A stored Cross Site Scripting (xss) vulnerability in the "content management" feature in AnQiCMS v.3.4.11 allows a remote attacker to execute arbitrary code via a crafted script to the title, categoryTitle, and tmpTag parameters. | Patched by core rule | Y |
| CVE-2025-7205 | CVE-2025 - The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored C... | The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the donor notes parameter in all versions up to, and including, 4.5.0 due to insufficient input sanitization and output | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | escaping. This makes it possible for authenticated attackers, with GiveWP worker-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Additionally, they need to trick an administrator into visiting the legacy version of the site. | | |
| CVE-2025-8370 | CVE-2025 - A vulnerability, which was classified as problematic, was found in Portabilis i-Educar 2.9. Affected... | A vulnerability, which was classified as problematic, was found in Portabilis i-Educar 2.9. Affected is an unknown function of the file /intranet/educar_escolaridade_lst.php. The manipulation of the argument descricao 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-2025-8369 | CVE-2025 - A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.9. Thi... | A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.9. This issue affects some unknown processing of the file /intranet/educar_avaliacao_desempenho_lst.php. The manipulation of the argument titulo_avaliacao 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-2025-8368 | CVE-2025 - A vulnerability classified as problematic was found in Portabilis i-Educar 2.9. This vulnerability a... | A vulnerability classified as problematic was found in Portabilis i-Educar 2.9. This vulnerability affects unknown code of the file /intranet/pesquisa_pessoa_lst.php. The manipulation of the argument campo_busca/cpf 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-2025-8367 | CVE-2025 - A | A vulnerability classified as | Patched by core | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | vulnerability classified as problematic has been found in Portabilis i-Educar 2.9. This affects an... | problematic has been found in Portabilis i-Educar 2.9. This affects an unknown part of the file /intranet/funcionario_vinculo_lst.php. The manipulation of the argument nome 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. | rule | |
| CVE-2025-8366 | CVE-2025 - A vulnerability was found in Portabilis i-Educar 2.9. It has been rated as problematic. Affected by ... | A vulnerability was found in Portabilis i-Educar 2.9. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /intranet/educar_servidor_lst.php. The manipulation of the argument nome/matricula_servidor 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. | Patched by core rule | Y |
| CVE-2025-5720 | CVE-2025 - The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripti... | The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author' parameter in all versions up to, and including, 5.80.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8365 | CVE-2025 - A vulnerability was found in Portabilis i-Educar 2.10. It has been declared as problematic. Affected... | A vulnerability was found in Portabilis i-Educar 2.10. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file atendidos_cad.php. The manipulation of the argument nome/nome_social/email 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 |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| CVE-2025-8346 | CVE-2025 - A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.10. Af... | A vulnerability, which was classified as problematic, has been found in Portabilis i-Educar 2.10. Affected by this issue is some unknown functionality of the file /educar_aluno_lst.php. The manipulation of the argument ref_cod_matricula with the input "><img%20src=x%20onerror=alert(%27CVE-Hunters%27)> 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. | Patched by core rule | Y |
| CVE-2025-8340 | CVE-2025 - A vulnerability was found in code-projects Intern Membership Management System 1.0. It has been decl... | A vulnerability was found in code-projects Intern Membership Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file fill_details.php of the component Error Message Handler. The manipulation of the argument email 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-2025-51954 | CVE-2025 - playground.electronhub.ai v1.1.9 was discovered to contain a cross-site scripting (XSS) vulnerabilit... | playground.electronhub.ai v1.1.9 was discovered to contain a cross-site scripting (XSS) vulnerability. | Patched by core rule | Y |
| CVE-2025-51951 | CVE-2025 - andisearch v0.5.249 was discovered to contain a cross-site scripting (XSS) vulnerability.... | andisearch v0.5.249 was discovered to contain a cross-site scripting (XSS) vulnerability. | Patched by core rule | Y |
| CVE-2025-5684 | CVE-2025 - The MetForm – Contact Form, Survey, Quiz, & Custom Form Builder for Elementor plugin for WordPress i... | The MetForm – Contact Form, Survey, Quiz, & Custom Form Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `mf-template` DOM Element in all versions up to, and including, 4.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | whenever a user accesses an injected page. | | |
| CVE-2025-44136 | CVE-2025 - MapTiler Tileserver-php v2.0 is vulnerable to Cross Site Scripting (XSS). The GET parameter "layer" ... | MapTiler Tileserver-php v2.0 is vulnerable to Cross Site Scripting (XSS). The GET parameter "layer" is reflected in an error message without html encoding. This leads to XSS and allows an unauthenticated attacker to execute arbitrary HTML or JavaScript code on a victim's browser. | Patched by core rule | Y |
| CVE-2025-52358 | CVE-2025 - A cross-site scripting vulnerability in Vivaldi United Group iCONTROL+ Server including Firmware ver... | A cross-site scripting vulnerability in Vivaldi United Group iCONTROL+ Server including Firmware version 4.7.8.0.eden Logic version 5.32 and below. This issue allows attackers to inject JavaScript payloads within the error or edit-menu-item parameters which are then executed in the victim's browser session. | Patched by core rule | Y |
| CVE-2025-8216 | CVE-2025 - The Sky Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via M... | The Sky Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Multiple widgets in all versions up to, and including, 3.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-8196 | CVE-2025 - The Magical Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting v... | The Magical Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Custom Attributes in all versions up to, and including, 1.3.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-4566 | CVE-2025 - The Elementor Website Builder – More Than Just a Page Builder plugin for | The Elementor Website Builder – More Than Just a Page Builder plugin for WordPress is vulnerable to | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | WordPress is vulnerable to ... | Stored Cross-Site Scripting via the data-text DOM element attribute in Text Path widget in all versions up to, and including, 3.30.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This attack affects only Chrome/Edge browsers | | |
| CVE-2025-3075 | CVE-2025 - The Elementor Website Builder – More Than Just a Page Builder plugin for WordPress is vulnerable to ... | The Elementor Website Builder – More Than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'elementor-element' shortcode in all versions up to, and including, 3.29.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only impacts sites with 'Element Caching' enabled. | Patched by core rule | Y |
| CVE-2025-7811 | CVE-2025 - The StreamWeasels YouTube Integration plugin for WordPress is vulnerable to Stored Cross-Site Script... | The StreamWeasels YouTube Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'data-uuid' attribute in all versions up to, and including, 1.4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-7810 | CVE-2025 - The StreamWeasels Kick Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting... | The StreamWeasels Kick Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'data-uuid' attribute in all versions up to, and including, 1.1.4 due to insufficient input sanitization and output escaping on user supplied | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |
| CVE-2025-7809 | CVE-2025 - The StreamWeasels Twitch Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripti... | The StreamWeasels Twitch Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'data-uuid' attribute in all versions up to, and including, 1.9.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-30125 | CVE-2025 - An issue was discovered on Marbella KR8s Dashcam FF 2.0.8 devices. All dashcams were shipped with th... | An issue was discovered on Marbella KR8s Dashcam FF 2.0.8 devices. All dashcams were shipped with the same default credentials of 12345678, which creates an insecure-by-default condition. For users who change their passwords, it's limited to 8 characters. These short passwords can be cracked in 8 hours via low-end commercial cloud resources. | Patched by core rule | Y |
| CVE-2025-8222 | CVE-2025 - A vulnerability, which was classified as problematic, has been found in jerryshensjf JPACookieShop 蛋... | A vulnerability, which was classified as problematic, has been found in jerryshensjf JPACookieShop 蛋糕商城 JPA版 up to 24a15c02b4f75042c9f7f615a3fed2ec1cefb999. Affected by this issue is some unknown functionality of the file GoodsController.java. The manipulation leads to cross site scripting. The attack may be launched 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. Multiple endpoints are affected. | Patched by core rule | Y |
| CVE-2025-8221 | CVE-2025 - A vulnerability classified as | A vulnerability classified as problematic was found in | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | problematic was found in jerryshensjf JPACookieShop 蛋糕商城JPA版 up to 24a... | jerryshensjf JPACookieShop 蛋糕商城JPA版 up to 24a15c02b4f75042c9f7f615a3fed2ec1cefb999. Affected by this vulnerability is the function goodsSearch of the file GoodsCustController.java. The manipulation of the argument keyword leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not available. | | |
| CVE-2025-8191 | CVE-2025 - A vulnerability, which was classified as problematic, was found in macrozheng mall up to 1.0.3. Affe... | A vulnerability, which was classified as problematic, was found in macrozheng mall up to 1.0.3. Affected is an unknown function of the file /swagger-ui/index.html of the component Swagger UI. The manipulation of the argument configUrl 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 deleted the GitHub issue for this vulnerability without any explanation. Afterwards the vendor was contacted early about this disclosure via email but did not respond in any way. | Patched by core rule | Y |
| CVE-2025-7501 | CVE-2025 - The Wonder Slider Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image t... | The Wonder Slider Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image title and description DOM in all versions up to, and including, 14.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | Patched by core rule | Y |
| CVE-2025-6987 | CVE-2025 - The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin... | The Advanced iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'advanced_iframe' shortcode in all versions up to, and including, 2025.5 due | Patched by core rule | Y |

| Public ID | Vulnerability Name | Vulnerability Description | AppTrana Coverage | Indusface WAS Coverage |
|---|---|---|---|---|
| | | to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. | | |

INDUSFACE™

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

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


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™