



WordPress EZPZ SAML SP Single Sign On (SSO) plugin <= 1.2.5 - CSRF to Stored XSS vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-24749
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-31 09:15:11 UTC
Updated	2026-04-28 19:29:31 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in Overt Software Solutions LTD EZPZ SAML SP Single Sign On (SSO) a

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from audit@patchstack.com

CVSS: 3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

EPSS: 0.001420000 probability, percentile 0.339470000 (date 2026-04-28)

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Overt Software Solutions LTD	EZPZ SAML SP Single Sign On SSO	affected n/a 1.2.5 custom	Not specified

References

Reference

[patchstack.com/database/wordpress/plugin/ezpz-sp/vulnerability/wordpress-ezpz...](https://patchstack.com/database/wordpress/plugin/ezpz-sp/vulnerability/wordpress-ezpz-sp-single-sign-on-sso-plugin-1-2-5-csrf-to-store)

<https://patchstack.com/database/wordpress/plugin/ezpz-sp/vulnerability/wordpress-ezpz-saml-sp-single-sign-on-sso-plugin-1-2-5-csrf-to-store>

[CVE Program record](#)

[NVD vulnerability detail](#)

Vendor Comments And Credit

Discovery Credit

CNA: SOPROBRO (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress EZPZ SAML SP Single Sign On (SSO) plugin to the latest available version (at least 1.2.6).

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report