



WordPress Sumo plugin <= 1.34 - Cross Site Request Forgery (CSRF) vulnerability

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2024-31265
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-12 13:15:17 UTC
Updated	2026-04-28 19:24:19 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in SumoMe Sumo.This issue affects Sumo: from n/a through 1.34.

Risk And Classification

Primary CVSS: v3.1 3.7 LOW from audit@patchstack.com

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

EPSS: 0.000470000 probability, percentile 0.145770000 (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	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	

None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SumoMe	Sumo	affected n/a 1.34 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/sumome/wordpress-sumo-plugin-1-34-cros...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Friday (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 1.35 or a higher version.

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