WordPress SAML Single Sign On – SSO Login plugin <= 5.0.4 - Broken Access Control vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-41873
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-13 15:15:25 UTC
Updated	2026-04-28 19:21:21 UTC
Description	Missing Authorization vulnerability in miniOrange SAML SP Single Sign On allows Exploiting Incorrectly Configured Access

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.001480000 probability, percentile 0.348790000 (date 2026-05-12)

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	MiniOrange	SAML SP Single Sign On	affected n/a 5.0.4 custom	Not specified

References

Reference
patchstack.com/database/wordpress/plugin/miniorange-saml-20-single-sign-on/v...
https://patchstack.com/database/wordpress/plugin/miniorange-saml-20-single-sign-on/vulnerability/wordpress-saml-single-sign-on-sso-login-pl
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: Abdi Pranata (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress SAML SP Single Sign On plugin to the latest available version (at least 5.0.5).

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 registred 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**