WordPress Simple Membership Plugin <= 4.3.8 is vulnerable to Unauth. Reflected Cross Site Scripting (XSS)

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

Summary

CVE	CVE-2023-50376
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-19 09:15:36 UTC
Updated	2026-04-28 19:22:32 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in smp7, wp.Insider Simp

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

EPSS: 0.001280000 probability, percentile 0.318150000 (date 2026-04-29)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
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

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple-membership-plugin	Simple Membership	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Smp7 Wp.insider	Simple Membership	affected n/a 4.3.8 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/simple-membership/wordpress-simple-mem...	af854a3a-2127-422b-91ae-364da2661108	patchstac
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Le Ngoc Anh (Patchstack Alliance) (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-12-11T01:41:00.000Z	Vulnerability received on the Patchstack Alliance bounty program.
CNA	2023-12-11T10:17:00.000Z	Vulnerability validated by Patchstack researchers.
CNA	2023-12-12T06:24:00.000Z	Patchstack notified the vendor about the vulnerability.
CNA	2023-12-13T10:45:00.000Z	Vendor confirmed that information was received.
CNA	2023-12-16T02:34:00.000Z	Vendor notified Patchstack that patched version is released.
CNA	2023-12-19T06:03:00.000Z	Patch validated, vulnerability disclosed to the Patchstack vulnerability database.

Solutions

CNA: Update to 4.3.9 or a higher version.

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

Free CVE JSON API cve.report/api

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