



String Locator <= 2.5.0 - Cross-Site Request Forgery to PHAR Deserialization

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

Summary

CVE	CVE-2022-2434
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-06 18:15:13 UTC
Updated	2026-04-08 17:16:45 UTC
Description	The String Locator plugin for WordPress is vulnerable to deserialization of untrusted input via the 'string-locator-path' param

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	security@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Instawp	String Locator	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Instawp	String Locator	affected 2.5.0 semver	Not specified

References

Reference	Source	Link
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wor
Vulnerability Advisories - Wordfence	af854a3a-2127-422b-91ae-364da2661108	www.wordfence
String Locator <= 2.5.0 - Cross-Site Request Forgery to PHAR Deserialization	af854a3a-2127-422b-91ae-364da2661108	www.wordfence
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wor
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Rasoul Jahanshahi (en)

Additional Advisory Data

Source	Time	Event
CNA	2022-08-08T00:00:00.000Z	Disclosed

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

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