



Slope Widgets <= 4.2.12 - Authenticated (Contributor+) Stored Cross-Site Scripting

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2024-11902
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-17 00:15:05 UTC
Updated	2026-04-08 18:19:35 UTC
Description	The Slope Widgets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'slope-reservations' sh

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from security@wordfence.com

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

EPSS: 0.002650000 probability, percentile 0.499870000 (date 2026-04-08)

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	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	Low
User Interaction	None
Scope	Changed
Confidentiality	

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Slopeit	Slope Widgets	affected 4.2.12 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/7700f1f3-90e2-450d-9cfe-c922d...	security@wordfence.com	www.wordfence.com
wordpress.org/plugins/slope-widgets	security@wordfence.com	wordpress.org
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpress.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Djaidja Moundjid (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-12-16T10:47:09.000Z	Disclosed

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

