Plezi <= 1.0.6 - Authenticated (Contributor+) Stored Cross-Site Scripting

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

Summary

CVE	CVE-2024-11763
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-14 05:15:07 UTC
Updated	2026-04-08 18:19:31 UTC
Description	The Plezi plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'plezi' shortcode in all versions u

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: 0.001720000 probability, percentile 0.385110000 (date 2026-04-15)

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	Plezi	Plezi	affected 1.0.6 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset/3209502/plezi/trunk/includes/plz-admin.php	security@wordfence.com	plugins.trac.wordpress.or
plugins.trac.wordpress.org/browser/plezi/trunk/includes/plz-admin.php	security@wordfence.com	plugins.trac.wordpress.or
www.wordfence.com/threat-intel/vulnerabilities/id/67768957-45be-48d9-ad5e-14729...	security@wordfence.com	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: SOPROBRO (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-12-13T00:00:00.000Z	Disclosed

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