Clio Grow <= 1.0.2 - Reflected Cross-Site Scripting

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

Summary

CVE	CVE-2024-8802
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-04 05:15:11 UTC
Updated	2026-04-08 17:19:40 UTC
Description	The Clio Grow plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg withou

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from security@wordfence.com

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

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	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

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	Clio	Clio Grow	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cliogrow	Clio Grow Form	affected 1.0.2 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/clio-grow-form/trunk/includes/class-grow-form-setting...	security@wordfence.com	plugins.trac.wordpre
www.wordfence.com/threat-intel/vulnerabilities/id/10fcfddf-0ed7-471d-86bf-c38e7...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpre
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: vgo0 (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-10-03T13:31:22.000Z	Disclosed

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**