ProfileGrid <= 5.5.1 - Authenticated (Subscriber+) Arbitrary Option Update

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

Summary

CVE	CVE-2023-3713
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-18 03:15:56 UTC
Updated	2026-04-08 18:18:11 UTC
Description	The ProfileGrid plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check or

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from security@wordfence.com

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

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

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

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Metagauss	Profilegrid	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Metagauss	ProfileGrid User Profiles Groups And Communities	affected 5.5.1 semver	Not specified

References

Reference	Source	Link
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wordpre
ProfileGrid <= 5.5.1 - Authenticated (Subscriber+) Arbitrary Option Update	af854a3a-2127-422b-91ae-364da2661108	www.wordfence.cor
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	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: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-06-23T00:00:00.000Z	Discovered
CNA	2023-06-25T00:00:00.000Z	Vendor Notified
CNA	2023-07-17T00:00:00.000Z	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 registred 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