ProfileGrid <= 5.5.0 - Hardcoded Encryption Key

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

Summary

CVE	CVE-2023-3404
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-31 06:15:09 UTC
Updated	2026-04-08 18:18:09 UTC
Description	The ProfileGrid plugin for WordPress is vulnerable to unauthorized decryption of private information in versions up to, and i

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from security@wordfence.com

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

Problem Types: CWE-321 | CWE-321 CWE-321 Use of Hard-coded Cryptographic Key

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

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 5.5.0 semver	Not specified

References

Reference	Source	Link	Tags
ProfileGrid <= 5.5.0 - Hardcoded Encryption Key	af854a3a-2127-422b-91ae-364da2661108	www.wordfence.com	Third Party Advi
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wordpress.org	Patch
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wordpress.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-06-25T00:00:00.000Z	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. 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**