



Grav: Administrative Account Disruption and Privilege De-escalation via User Overwrite Logic

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-42609
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 16:17:33 UTC
Updated	2026-05-12 16:16:54 UTC
Description	Grav is a file-based Web platform. Prior to 2.0.0-beta.2, a business logic vulnerability in the Grav Admin Panel allows a low-

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from security-advisories@github.com

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

EPSS: 0.000390000 probability, percentile 0.116460000 (date 2026-05-12)

Problem Types: CWE-269 | CWE-285 | CWE-639 | CWE-837 | CWE-269 CWE-269: Improper Privilege Management | CWE-285 CWE-285: Improper Authorization | CWE-639 CWE-639: Authorization Bypass Through User-Controlled Key | CWE-837 CWE-837: Improper Enforcement of a Single, Unique Action

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
3.1	CNA	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Getgrav	Grav	2.0.0	beta1	All	All
Application	Getgrav	Grav	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Getgrav	Grav	affected < 2.0.0-beta.2	Not specified

References

Reference	Source	Link	Tags
github.com/getgrav/grav/commit/d904efc33e03ebb597afde8d3368b28cf0423632	security-advisories@github.com	github.com	Patch
github.com/getgrav/grav/security/advisories/GHSA-rr73-568v-28f8	security-advisories@github.com	github.com	Exploit
github.com/getgrav/grav/commit/5a12f9be8314682c8713e569e330f11805d0a663	security-advisories@github.com	github.com	Patch
github.com/getgrav/grav/commit/c66dfeb5ff679a1667678c6335eb9ff3255dfc47	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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