



Grav: Remote Code Execution (RCE) via Malicious Plugin ZIP Upload in Direct Install Feature

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

Summary

CVE	CVE-2026-42607
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 16:17:32 UTC
Updated	2026-05-12 14:51:21 UTC
Description	Grav is a file-based Web platform. Prior to 2.0.0-beta.2, an authenticated user with administrative privileges can achieve R

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from security-advisories@github.com

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

EPSS: 0.002330000 probability, percentile 0.460330000 (date 2026-05-12)

Problem Types: CWE-94 | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

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

References

Reference	Source	Link
github.com/getgrav/grav/security/advisories/GHSA-w48r-jppp-rcfw	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/getgrav/grav/commit/5a12f9be8314682c8713e569e330f11805d0a663	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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