grav-plugin-admin: Stored Cross-Site Scripting (XSS) Reflected endpoint /admin/pages/[page], parameter data[header][title]

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

Summary

CVE	CVE-2026-44737
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 17:16:34 UTC
Updated	2026-05-11 20:25:46 UTC
Description	grav-plugin-admin is the admin plugin for Grav is an HTML user interface that provides a convenient way to configure Grav

Risk And Classification

Primary CVSS: v4.0 6.2 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:L/VI:L/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

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
4.0	security-advisories@github.com	Secondary	6.2	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:L/VI:L/VA:N/SC:H/S
4.0	CNA	DECLARED	6.2	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:L/VI:L/VA:N/SC:H/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Active

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:L/VI:L/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Getgrav	Grav-plugin-admin	affected < 1.10.49.5	Not specified

References

Reference	Source	Link
github.com/getgrav/grav-plugin-admin/commit/f67cc18e81d8767bb43d29ee6422...	security-advisories@github.com	github.com
github.com/getgrav/grav/security/advisories/GHSA-fmg2-f5r9-24qc	134c704f-9b21-4f2e-91b3-4a467353bcc0	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.