WordPress Countdown Widget plugin <= 3.1.9.1 - Cross-Site Request Forgery (CSRF) leading to Cross-Site Scripting (XSS)

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

Summary

CVE	CVE-2022-45847
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-27 14:15:08 UTC
Updated	2026-04-28 19:19:04 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in WPAssist.Me WordPress Countdown Widget allows Cross-Site Scriptin

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpassist	Countdown Widget	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WPAssist.me	WordPress Countdown Widget	affected n/a 3.1.9.1 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/wordpress-countdown-widget/wordpress-c...	af854a3a-2127-422b-91ae-364da2661108	patchstack
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

Vendor Comments And Credit

Discovery Credit

CNA: Rasi Afeef (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 3.1.9.3 or a higher version.

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