WordPress Pinterest Plugin <= 1.8.2 - Cross Site Scripting (XSS)

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

Summary

CVE	CVE-2024-30192
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-27 07:15:54 UTC
Updated	2026-04-28 19:23:56 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GS Plugins GS Pins fo

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from ADP

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

EPSS: 0.001330000 probability, percentile 0.324520000 (date 2026-04-28)

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
3.1	ADP	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	audit@patchstack.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.9	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gsplugins	Gs Pinterest Portfolio	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GS Plugins	GS Pins For Pinterest	affected n/a 1.8.2 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/gs-pinterest-portfolio/wordpress-pinte...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
patchstack.com/database/Wordpress/Plugin/gs-pinterest-portfolio/vulnerabilit...	MITRE	patchstack.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: LVT-tholv2k (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 1.8.3 or a higher version.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report