WordPress wpForo plugin <= 2.2.5 - Broken Access Control + CSRF vulnerability

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

Summary

CVE	CVE-2023-47869
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-09 13:15:32 UTC
Updated	2026-04-23 15:17:52 UTC
Description	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in gVectors Team wpForo F

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov

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

EPSS: 0.001890000 probability, percentile 0.403790000 (date 2026-05-12)

Problem Types: CWE-80 | CWE-79 | CWE-80 CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/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	Gvectors	Wpforo Forum	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GVectors Team	WpForo Forum	affected n/a 2.2.5 custom	Not specified

References

Reference	Source
patchstack.com/database/wordpress/plugin/wpforo/vulnerability/wordpress-wpfo...	https://patchstack.com/database/wordpress/plugin/wpforo
patchstack.com/database/Wordpress/Plugin/wpforo/vulnerability/wordpress-wpfo...	audit@patchstack.com
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Jesse McNeil (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: No patched version is available. No reply from the vendor.

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