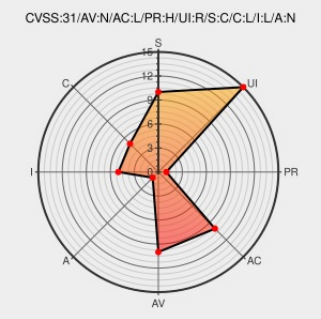
CVE-2022-44736

Published on: Not Yet Published

Last Modified on: 11/18/2022 07:29:00 PM UTC

CVE-2022-44736

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Chameleon from Chameleon Project contain the following vulnerability:

Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Chameleon plugin <= 1.4.3 on WordPress.

CVE-2022-44736 has been assigned by audit@patchstack.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Fahad Mahmood** - **Chameleon (WordPress plugin)** version **<= 1.4.3**

CVSS3 Score: 4.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
WordPress Chameleon plugin <= 1.4.3 - Auth. Stored Cross-Site Scripting (XSS) vulnerability - Patchstack	patchstack.com text/html	CONFIRM patchstack.com/database/vulnerability/chameleon/wordpress-chameleon-plugin-1-4-3-auth-stored-cross-site-scripting-xss-vulnerability?_s_id=cve

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Chameleon Project	Chameleon	All	All	All	All

cpe:2.3:a:chameleon_project:chameleon:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Vulnerability discovered by Hoang Van Hiep aka sk4rl1ghT (Patchstack Alliance)

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-44736 : Auth. admin+ Stored Cross-Site Scripting #XSS vulnerability in Chameleon plugin <= 1.4.3 on Wo… twitter.com/i/web/status/1…	2022-11-17 23:17:25
@LinInfoSec	Wordpress - CVE-2022-44736: patchstack.com/database/vulne…	2022-11-18 02:00:21
/r/netcve	CVE-2022-44736	2022-11-18 00:39:06

← Previous ID

Next ID→