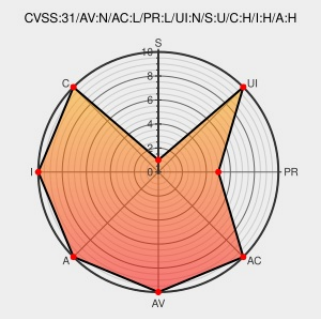
CVE-2021-24626

Published on: 11/08/2021 12:00:00 AM UTC

Last Modified on: 11/09/2022 09:43:00 PM UTC

CVE-2021-24626

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



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

The Chameleon CSS WordPress plugin through 1.2 does not have any CSRF and capability checks in all its AJAX calls, allowing any authenticated user, such as subscriber to call them and perform unauthorised actions. One of AJAX call, remove_css, also does not sanitise or escape the css_id POST parameter before using it in a SQL statement, leading to a SQL Injection

CVE-2021-24626 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Unknown** - **Chameleon CSS** version **<= 1.2**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Attention Required! | Cloudflare	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/06cb6c14-99b8-45b6-be2e-f4dcca8a4165
wp-plugin : chameleon-css | Code Vigilant : to err is human.. To fix is Humanity	codevigilant.com text/html	MISC codevigilant.com/disclosure/2021/wp-plugin-chameleon-css/

There are currently no QIDs associated with this CVE

Exploit/POC from Github

The Chameleon CSS WordPress plugin through 1.2 does not have any CSRF and capability checks in all its AJAX calls, al…

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:chameleon_css_project:chameleon_css:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Shreya Pohekar of Codevigilant Project

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-24626 : The Chameleon CSS WordPress plugin through 1.2 does not have any CSRF and capability checks in all… twitter.com/i/web/status/1…	2021-11-08 17:48:11

← Previous ID

Next ID→