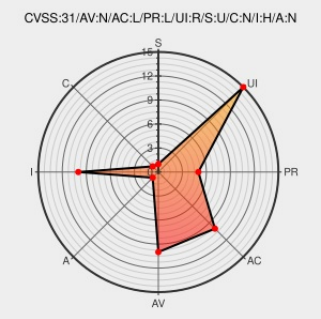
CVE-2021-24752

Published on: 10/18/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 03:32:00 PM UTC

CVE-2021-24752

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



Certain versions of Catch Scroll Progress Bar from Catchplugins contain the following vulnerability:

Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_switch AJAX action, which could allow any authenticated users, such as Subscriber to change the Essential Widgets WordPress plugin before 1.9, To Top WordPress plugin before 2.3, Header Enhancement WordPress plugin before 1.5, Generate Child Theme WordPress plugin before 1.6, Essential Content Types WordPress plugin before 1.9, Catch Web Tools WordPress plugin before 2.7, Catch Under Construction WordPress plugin before 1.4, Catch Themes Demo Import WordPress plugin before 1.6, Catch Sticky Menu WordPress plugin before 1.7, Catch Scroll Progress Bar WordPress plugin before 1.6, Social Gallery and Widget WordPress plugin before 2.3, Catch Infinite Scroll WordPress plugin before 1.9, Catch Import Export WordPress plugin before 1.9, Catch Gallery WordPress plugin before 1.7, Catch Duplicate Switcher WordPress plugin before 1.6, Catch Breadcrumb WordPress plugin before 1.7, Catch IDs WordPress plugin before 2.4's configurations.

CVE-2021-24752 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.7 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Attention Required! | Cloudflare	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/181a729e-fffe-457c-9e8d-a4343fd2e630

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Catchplugins	Catch Scroll Progress Bar	All	All	All	All
Application	Catchplugins	Catch Sticky Menu	All	All	All	All
Application	Catchplugins	Catch Themes Demo Import	All	All	All	All
Application	Catchplugins	Catch Under Construction	All	All	All	All
Application	Catchplugins	Catch Web Tools	All	All	All	All
Application	Catchplugins	Essential Content Types	All	All	All	All
Application	Catchplugins	Essential Widgets	All	All	All	All
Application	Catchplugins	Generate Child Theme	All	All	All	All
Application	Catchplugins	Header Enhancement	All	All	All	All
Application	Catchplugins	To Top	All	All	All	All

cpe:2.3:a:catchplugins:catch_scroll_progress_bar:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:catch_sticky_menu:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:catch_themes_demo_import:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:catch_under_construction:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:catch_web_tools:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:essential_content_types:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:essential_widgets:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:generate_child_theme:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:header_enhancement:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:catchplugins:to_top:*:*:*:*:*:wordpress:*:*:

Discovery Credit

apple502j

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-24752 : Multiple Plugins from the CatchThemes vendor do not perform capability and CSRF checks in the ctp_… twitter.com/i/web/status/1…	2021-10-18 14:01:51

← Previous ID

Next ID→