

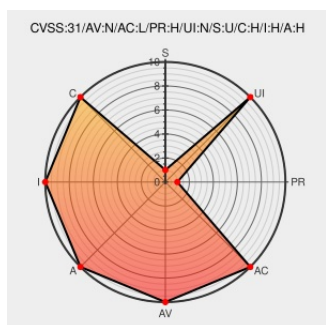


CVE-2021-39352

Published on: 10/21/2021 12:00:00 AM UTC

Last Modified on: 02/28/2022 02:59:00 PM UTC

CVE-2021-39352

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Catch Themes Demo Import](#) from [Catchplugins](#) contain the following vulnerability:

The Catch Themes Demo Import WordPress plugin is vulnerable to arbitrary file uploads via the import functionality found in the `~/inc/CatchThemesDemoImport.php` file, in versions up to and including 1.7, due to insufficient file type validation. This makes it possible for an attacker with administrative privileges to upload malicious files that can be used to achieve remote code execution.

CVE-2021-39352 has been assigned by security@wordfence.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Catch Themes Demo Import - Catch Themes Demo Import** version `<= 1.7`

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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
-------------	------	------

403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/changeset/2617555/catch-themes-demo-import/trunk/inc/CatchThemesDemoImport.php
Exploits/Wordpress/CVE-2021-39352 at main · Hacker5preme/Exploits · GitHub	github.com text/html	MISC github.com/Hacker5preme/Exploits/tree/main/Wordpress/CVE-2021-39352
Wordpress Plugin Catch Themes Demo Import 1.6.1 - Remote Code Execution (RCE) (Authenticated) - PHP webapps Exploit	www.exploit-db.com Proof of Concept text/html	MISC www.exploit-db.com/exploits/50580
word-press/Catch Themes Demo Import.md at main · BigTiger2020/word-press · GitHub	github.com text/html	MISC github.com/BigTiger2020/word-press/blob/main/Catch%20Themes%20Demo%20Import.md
WordPress Catch Themes Demo Import 1.6.1 Shell Upload ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/165207/WordPress-Catch-Themes-Demo-Import-1.6.1-Shell-Upload.html
Vulnerability Advisories - Wordfence	www.wordfence.com text/html	MISC www.wordfence.com/vulnerability-advisories/#CVE-2021-39352
WordPress Catch Themes Demo Import Shell Upload ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/165463/WordPress-Catch-Themes-Demo-Import-Shell-Upload.html

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Catchplugins	Catch Themes Demo Import	All	All	All	All
cpe:2.3:a:catchplugins:catch_themes_demo_import:*:*:*:*:wordpress:*:*						

Discovery Credit

Thinkland Security Team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39352 : The Catch Themes Demo Import WordPress plugin is vulnerable to arbitrary file uploads via the impo... twitter.com/i/web/status/1...	2021-10-21 20:05:49
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-39352 Description: The Catch Themes Demo Import WordPress plugin is vul... twitter.com/i/web/status/1...	2021-10-21 21:00:10
@LinInfoSec	Wordpress - CVE-2021-39352: plugins.trac.wordpress.org/changeset/2617...	2021-10-28 00:21:36

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)