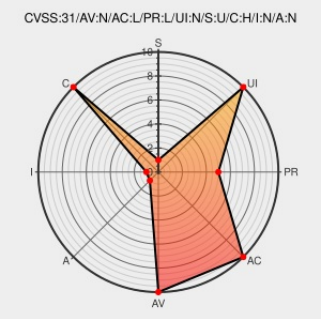
CVE-2021-4332

Published on: Not Yet Published

Last Modified on: 03/14/2023 08:49:00 PM UTC

CVE-2021-4332

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



Certain versions of The Plus Addons For Elementor from Posimyth contain the following vulnerability:

The Plus Addons for Elementor plugin for WordPress is vulnerable to arbitrary file reads in versions up to, and including 4.1.9 (pro) and 2.0.6 (free). The plugin has a feature to add an "Info Box" to an Elementor created page. This Info Box can include an SVG image for the box. Unfortunately, the plugin used file_get_contents with no verification that the file being supplied was an SVG file, so any user with access to the Elementor page builder, such as contributors, could read arbitrary files on the WordPress installation.

CVE-2021-4332 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **posimythemes** - **The Plus Addons for Elementor | FREE Elementor Widgets & Elementor Templates, Header Menu, Blog Post Builder, Dark Mode, Full-Page Scroll, Cross Domain Copy** version **<= 2.0.6**

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
The Plus Addons for Elementor PRO <= 4.1.9 & The Plus Addons for Elementor <= 2.0.6 - Authenticated (Contributor+) Arbitrary File Read	www.wordfence.com text/html	MISC www.wordfence.com/threat-intel/vulnerabilities/id/aa698e7e-b1c7-4ead-aa2e-7fbfc9dfac80
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2523506%40the-plus-addons-for-elementor-page-builder&new=2523506%40the-plus-addons-for-elementor-

page-builder&sfp_email=&sfph_mail=

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	Posimyth	The Plus Addons For Elementor	All	All	All	All
Application	Posimyth	The Plus Addons For Elementor	All	All	All	All

cpe:2.3:a:posimyth:the_plus_addons_for_elementor:*:*:*:*:free:wordpress:*:*:

cpe:2.3:a:posimyth:the_plus_addons_for_elementor:*:*:*:*:pro:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@fjullien06	This is how I bypassed the Renesas RX65 protection: collshade.fr/articles/renes… It's been assigned a CVE (CVE-2021-4332… twitter.com/i/web/status/1…	2021-12-02 21:39:45
@ipssignatures	The vuln CVE-2021-4332 has a tweet created 0 days ago and retweeted 12 times. twitter.com/fjullien06/sta… #pow1rtrtwwcve	2021-12-03 16:06:00
@CVEreport	CVE-2021-4332 : The Plus Addons for Elementor plugin for WordPress is vulnerable to arbitrary file reads in version… twitter.com/i/web/status/1…	2023-03-07 15:08:20
/r/netcve	CVE-2021-4332	2023-03-07 15:40:56

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report