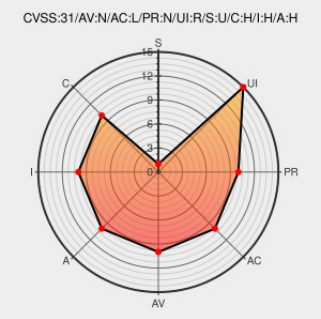
CVE-2021-24620

Published on: 09/13/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 06:13:00 PM UTC

CVE-2021-24620

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



Certain versions of Simple-e-commerce-shopping-cart from Simple-e-commerce-shopping-cart Project contain the following vulnerability:

The WordPress Simple Ecommerce Shopping Cart Plugin- Sell products through Paypal plugin through 2.2.5 does not check for the uploaded Downloadable Digital product file, allowing any file, such as PHP to be uploaded by an administrator. Furthermore, as there is no CSRF in place, attackers could also make a logged admin upload a malicious PHP file, which would lead to RCE

CVE-2021-24620 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Unknown** - **WordPress Simple Ecommerce Shopping Cart Plugin- Sell products through Paypal** version **<= 2.2.5**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Description	Tags	Link
Attention Required! | Cloudflare	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/1f2b3c4a-f7e9-4d22-b71e-f6b051fd8349

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

PoC for exploiting CVE-2021-24620 : The WordPress Simple Ecommerce Shopping Cart Plugin- Sell products through Paypal…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simple-e-commerce-shopping-cart Project	Simple-e-commerce-shopping-cart	All	All	All	All

cpe:2.3:a:simple-e-commerce-shopping-cart_project:simple-e-commerce-shopping-cart:*:*:*:*:*:wordpress:*:*:

Discovery Credit

h3v0x

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Wordpress - CVE-2021-24620: wpscan.com/vulnerability/…	2021-09-13 20:48:27

← Previous ID

Next ID→