



CVE-2022-42698

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-42698
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-18 23:15:00 UTC
Updated	2022-11-21 19:32:00 UTC
Description	Unauth. Arbitrary File Upload vulnerability in WordPress Api2Cart Bridge Connector plugin <= 1.1.0 on WordPress.

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Api2cart	Api2cart Bridge Connector	1.0.0	All	All	All
Application	Api2cart	Api2cart Bridge Connector	1.1.0	All	All	All

References

Reference	Source	Link	Tags
WordPress Api2Cart Bridge Connector plugin <= 1.1.0 - Arbitrary File Upload vulnerability - Patchstack	CONFIRM	patchstack.com	
Api2Cart Bridge Connector – WordPress plugin WordPress.org	CONFIRM	wordpress.org	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

Vendor Comments And Credit

Discovery Credit

LEGACY: Vulnerability discovered by Dave Jong (Patchstack)

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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