



CVE-2020-29471

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

Summary

CVE	CVE-2020-29471
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-29 17:15:00 UTC
Updated	2020-12-30 16:42:00 UTC
Description	OpenCart 3.0.3.6 is affected by cross-site scripting (XSS) in the Profile Image. An admin can upload a profile image as a m

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opencart	Opencart	3.0.3.6	All	All	All
Application	Opencart	Opencart	3.0.3.6	All	All	All

References

Reference	Source	Link	T
OpenCart 3.0.3.6 - 'Profile Image' Stored Cross Site Scripting (Authenticated) - PHP webapps Exploit	MISC	www.exploit-db.com	E
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

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