



CVE-2022-40407

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

Summary

CVE	CVE-2022-40407
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-29 14:15:00 UTC
Updated	2022-10-04 12:57:00 UTC
Description	A zip slip vulnerability in the file upload function of Chamilo v1.11 allows attackers to execute arbitrary code via a crafted Zip

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Chamilo	Chamilo	1.11	All	All	All

References

Reference	Source	Link
Security issues - Chamilo LMS - Chamilo Tracking System	CONFIRM	support.chamilo.org
GitHub - chamilo/chamilo-lms: Chamilo is a learning management system focused on ease of use and accessibility	MISC	github.com
security-research/ChamiloRceViaZipSlip.md at main · alexmackey/security-research · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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