



CVE-2022-0705

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

Summary

CVE	CVE-2022-0705
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-16 11:15:00 UTC
Updated	2022-03-22 15:22:00 UTC
Description	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pimcore	Pimcore	All	All	All	All

References

Reference	Source	Link
[Admin] Security - Add handler to enable Content Security Policy (#11... · pimcore/pimcore@6e0922c · GitHub	MISC	github.com
Cross-site Scripting (XSS) - Stored vulnerability found in pimcore	CONFIRM	huntr.dev
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.

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