



CVE-2021-4084

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

Summary

CVE	CVE-2021-4084
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-10 12:15:00 UTC
Updated	2021-12-13 19:28:00 UTC
Description	pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

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 UI] DataObject Class - escape general settings input values (#... · pimcore/pimcore@3c2a14e · 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