Pimcore Platform v12.3.3 - Stored XSS in Document Editable Embed rendering

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-5362
State	PUBLISHED
Assigner	Fluid Attacks
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-27 21:16:42 UTC
Updated	2026-04-28 20:11:56 UTC
Description	An authenticated attacker with permission to edit document content can store crafted HTML/JavaScript in a Document emb

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from help@fluidattacks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000020000 probability, percentile 0.000320000 (date 2026-04-28)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	help@fluidattacks.com	Secondary	4.8	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Active

Active

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pimcore	Pimcore	affected v12.3.3	Windows, MacOS, Linux

References

Reference	Source	Link	Tags
github.com/pimcore/pimcore	help@fluidattacks.com	github.com	
fluidattacks.com/es/advisories/mago	help@fluidattacks.com	fluidattacks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Oscar Naveda (en)

CNA: Fluid Attacks' AI SAST Scanner (en)

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

Free CVE JSON API cve.report/api

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