



# Pimcore Platform v12.3.3 - SQL Injection in DataObject composite index handling

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

## Summary

<b>CVE</b>	CVE-2026-5394
<b>State</b>	PUBLISHED
<b>Assigner</b>	Fluid Attacks
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-27 20:16:28 UTC
<b>Updated</b>	2026-05-05 18:16:03 UTC
<b>Description</b>	An authenticated administrative user who can import or save DataObject class definitions can inject attacker-controlled cor

## Risk And Classification

**Primary CVSS:** v4.0 7 HIGH from help@fluidattacks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000130000 probability, percentile 0.019950000 (date 2026-05-05)

**Problem Types:** CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
4.0	help@fluidattacks.com	Secondary	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N/E::
4.0	CNA	CVSS	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

None

Confidentiality

High

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/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/MSX/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 12.3.3	Windows, MacOS, Linux

### References

Reference	Source	Link	Tags
github.com/pimcore/pimcore	help@fluidattacks.com	github.com	
fluidattacks.com/es/advisories/dragons	help@fluidattacks.com	fluidattacks.com	
github.com/pimcore/pimcore/pull/19108	help@fluidattacks.com	github.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.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)