SQL Injection in pimcore/pimcore

0

✓ Valid Reported on Jan 9th 2022

Description

The `storeId` parameter does not sanitise and escape the option parameter before using it in a SQL statement, which could lead to SQL injection.

Proof of Concept

Add items to Classification Store: Key definition, Group,...
Injection (boolean base):

```
https://demo.pimcore.fun/admin/classificationstore/properties?
_dc=1639830472106&storeId=1))+and+((1=2&page=1&start=0&limit=25
```

Impact

A successful attack may result the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, write file to server lead to Remote code Execute, or write script to extract data

Occurrences

ClassificationstoreController.php L1245

CVE
CVE-2022-0258
(Published)

Vulnerability Type
CWE-89: SQL Injection

Severity
High (8.3)

Visibility

Visibility
Public

Status
Fixed

Found by

laladee
@laladee
unranked

Fixed by

Bernhard Rusch
@brusch
maintainer

This report was seen 494 times.

We are processing your report and will contact the **pimcore** team within 24 hours. a year ago

We have contacted a member of the **pimcore** team and are waiting to hear back a year ago

We have sent a follow up to the **pimcore** team. We will try again in 7 days. 10 months ago

Bernhard Rusch validated this vulnerability 10 months ago

laladee has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bernhard Rusch marked this as fixed with commit **66281c** 10 months ago

Bernhard Rusch has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

ClassificationstoreController.php#L1245 has been validated ✓

Chat with us

Sign in to join this conversation