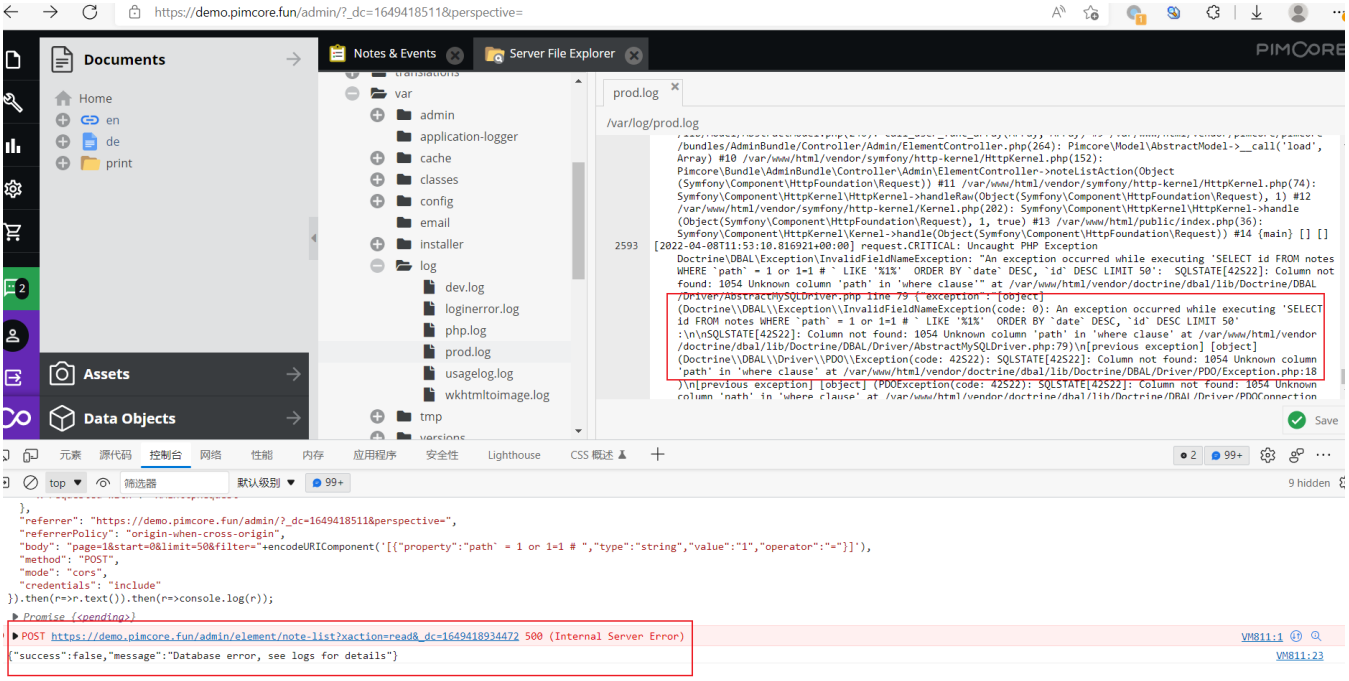
SQL injection in ElementController.php in pimcore/pimcore

0

Valid Reported on Apr 8th 2022

Description

The property parameter is append to the sql query directly, which leads to a sql injection problem. if you set a wrong value. you can see the error from log.



then you can check the result.

after injection

Proof of Concept

// PoC.js

```
"body": "filterText=sdf&page=1&start=0&limit=50&filter="+encodeURIComponent
```

Impact

This vulnerability is capable of steal the data

Occurrences

ElementController.php L249

Chat with us

CVE

CVE-2022-1339

(Published)

Vulnerability Type
CWE-89: SQL Injection

Severity
High (8.8)

Registry
Packagist

Affected Version
10.3.4

Visibility
Public

Status
Fixed

Found by

mylong
@mylong
unranked

Fixed by

aryaantony92
@aryaantony92
maintainer

This report was seen 833 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 8 months ago

mylong modified the report 8 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 8 months ago

A **pimcore/pimcore** maintainer has acknowledged this report 8 months ago

aryaantony92 validated this vulnerability 7 months ago

mylong has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

aryaantony92 marked this as fixed in 10.3.5 with commit adae3b 7 months ago

aryaantony92 has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

ElementController.php#L249 has been validated ✔

mylong 7 months ago Researcher

Hi,@aryaantony92. the fixup in line 245. `$dateCondition = '`' . $filter[$propertyKey] . '` ' . ' BETWEEN ' . $db->quote($value) . ' AND ' . $db->quote($maxTime);` may be the `$filter[$propertyKey]` should also be quoted?

Sign in to join this conversation

terms

privacy policy

Chat with us