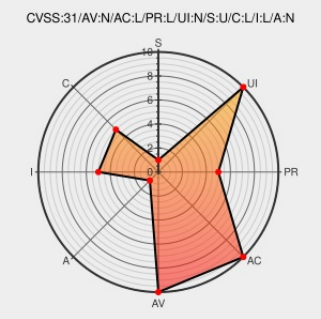
CVE-2023-23937

Published on: Not Yet Published

Last Modified on: 02/13/2023 03:21:00 PM UTC

CVE-2023-23937 - advisory for GHSA-8xv4-jj4h-qww6

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pimcore from Pimcore contain the following vulnerability:

Pimcore is an Open Source Data & Experience Management Platform: PIM, MDM, CDP, DAM, DXP/CMS & Digital Commerce. The upload functionality for updating user profile does not properly validate the file content-type, allowing any authenticated user to bypass this security check by adding a valid signature (p.e. GIF89) and sending any invalid content-type. This could allow an authenticated attacker to upload HTML files with JS content that will be executed in the context of the domain. This issue has been patched in version 10.5.16.

CVE-2023-23937 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **pimcore** - **pimcore** version **= < 10.5.16**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
Missing file upload type validation in user profile · Advisory · pimcore/pimcore · GitHub	github.com text/html	MISC github.com/pimcore/pimcore/security/advisories/GHSA-8xv4-jj4h-qww6
[Task]: Mime type check on Profile Avatar upload (#14125) · pimcore/pimcore@75a448e · GitHub	github.com text/html	MISC github.com/pimcore/pimcore/commit/75a448ef8ac74424cf4e723afeb6d05f9eed872f

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Pimcore is an Open Source Data & Experience Management Platform: PIM, MDM, CDP, DAM, DXP/CMS & Digital Commerce. The …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pimcore	Pimcore	All	All	All	All

cpe:2.3:a:pimcore:pimcore:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2023-23937	2023-02-03 20:38:51

← Previous ID

Next ID→