



CVE-2022-46157

Published on: Not Yet Published

Last Modified on: 12/14/2022 03:08:00 PM UTC

CVE-2022-46157 - advisory for GHSA-w9wc-4xcq-8gr6

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Product Information Management](#) from [Akeneo](#) contain the following vulnerability:

Akeneo PIM is an open source Product Information Management (PIM). Akeneo PIM Community Edition versions before v5.0.119 and v6.0.53 allows remote authenticated users to execute arbitrary PHP code on the server by uploading a crafted image. Akeneo PIM Community Edition after the versions aforementioned provides patched

Apache HTTP server configuration file, for docker setup and in documentation sample, to fix this vulnerability. Community Edition users must change their Apache HTTP server configuration accordingly to be protected. The patch for Cloud Based Akeneo PIM Services customers has been applied since 30th October 2022. Users are advised to upgrade. Users unable to upgrade may Replace any reference to `` in their apache httpd configurations with: `

CVE-2022-46157 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [akeneo](#) - **pim-community-dev** version = **>= 6.0.0, < 6.0.53**

Affected Vendor/Software: [akeneo](#) - **pim-community-dev** version = **< 5.0.119**

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
-------------	------	------

Remote php code execution · Advisory · akeneo/pim-community-dev · GitHub

github.com

text/html

MISC github.com/akeneo/pim-community-dev/security/advisories/GHSA-w9wc-4xcq-8gr6

pim-community-dev/httpd.conf at b4d79bb073c8b68ea26ab227c97cc78d86c4cba1 · akeneo/pim-community-dev · GitHub

github.com

text/html

MISC github.com/akeneo/pim-community-dev/blob/b4d79bb073c8b68ea26ab227c97cc78d86c4cba1/docker/httpd.conf

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Akeneo	Product Information Management	All	All	All	All

cpe:2.3:a:akeneo:product_information_management:***:community:***:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-46157 : Akeneo PIM is an open source Product Information Management PIM . Akeneo PIM Community Edition ve... twitter.com/i/web/status/1...	2022-12-09 21:03:29
/r/netcve	CVE-2022-46157	2022-12-09 22:41:18

← Previous ID

Next ID →