



CVE-2021-4139

Published on: Not Yet Published

Last Modified on: 01/07/2022 03:14:00 PM UTC

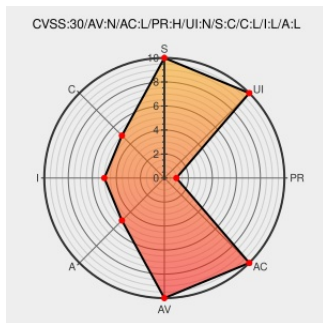
CVE-2021-4139 - advisory for 6ec59e43-095f-4ba3-8b75-e92250da8e3a

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Pimcore](#) from [Pimcore](#) contain the following vulnerability:

pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVE-2021-4139 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **pimcore** - pimcore/pimcore version < 10.2.7

CVSS3 Score: **9 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
huntr – the Bug Bounty Platform for any GitHub repository	huntr.dev text/html Inactive Link Not Archived	CONFIRM huntr.dev/bounties/6ec59e43-095f-4ba3-8b75-e92250da8e3a

Repository

[Classification Store]

Properly escape values on grids & titles · pimcore/pimcore@d5c3e87 · GitHub

github.com

text/html

MISC

github.com/pimcore/pimcore/commit/d5c3e876d910784000335061c3bd24d301351

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	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)
@huntrHacktivity	Cross-site Scripting (XSS) - Stored in github.com/pimcore/pimcore (CVE-2021-4139) reported by laladee - Patch:... twitter.com/i/web/status/1...	2021-12-21 09:01:36
@CVEreport	CVE-2021-4139 : pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation 'Cross-site S... twitter.com/i/web/status/1...	2021-12-21 12:54:39
@OpenSourceHacks	(CVE-2021-4139): Cross-site Scripting (XSS) - Stored in pimcore/pimcore. Disclosed by huntr.dev/users/laladee , fix... twitter.com/i/web/status/1...	2021-12-21 13:46:54
/r/netcve	CVE-2021-4139	2021-12-21 13:38:30

← Previous ID

Next ID →