



CVE-2021-4081

Published on: 12/10/2021 12:00:00 AM UTC

Last Modified on: 12/10/2021 11:06:00 PM UTC

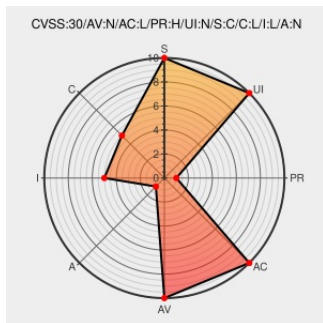
CVE-2021-4081 - advisory for da173e66-76ba-4f98-b8fb-429aabf222d3

[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-2021-4081 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **pimcore** - pimcore/pimcore version < 10.2.6

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

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/da173e66-76ba-4f98-b8fb-429aabf222d3

Repository

[Admin UI] Escape query on Search Window · pimcore/pimcore@34ed0e0 · GitHub

github.com

text/html

MISC

github.com/pimcore/pimcore/commit/34ed0e050ff679b4b38414aef48ea1ff956f907e

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) - Reflected in github.com/pimcore/pimcore (CVE-2021-4081) reported by @khanhchauminh - Patc... twitter.com/i/web/status/1...	2021-12-09 11:01:28
@CVEreport	CVE-2021-4081 : pimcore is vulnerable to Improper Neutralization of Input During Web Page Generation 'Cross-site S... twitter.com/i/web/status/1...	2021-12-10 10:32:31
@OpenSourceHacks	(CVE-2021-4081): Cross-site Scripting (XSS) - Reflected in pimcore/pimcore. Disclosed by @khanhchauminh, fixed by... twitter.com/i/web/status/1...	2021-12-10 11:17:55
/r/netcve	CVE-2021-4081	2021-12-10 11:38:25

← Previous ID

Next ID →

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)