

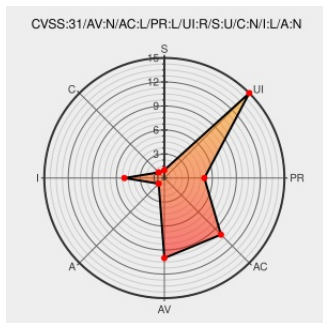


CVE-2022-4514

Published on: Not Yet Published

Last Modified on: 12/20/2022 09:13:00 PM UTC

CVE-2022-4514

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

Certain versions of [Oc-server3](#) from [Opencaching](#) contain the following vulnerability:

A vulnerability, which was classified as problematic, was found in Opencaching Deutschland oc-server3. Affected is an unknown function of the file htdocs/lang/de/ocstyle/varset.inc.php. The manipulation of the argument varvalue leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the

public and may be used. The name of the patch is

4bdd6a0e7b7760cea03b91812cbb80d7b16e3b5f. It is recommended to apply a patch to fix this issue. VDB-215886 is the identifier assigned to this vulnerability.

CVE-2022-4514 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Opencaching Deutschland](#) - **oc-server3** version **n/a**

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

CVE References

Description	Tags	Link
Fix XSS from open bug bounty from slack message 01 by sdenner · Pull Request #902 · OpencachingDeutschland/oc-server3 · GitHub	github.com text/html	MISC github.com/OpencachingDeutschland/oc-server3/pull/902
Merge pull request #902 from sdenner/fix/open-bug-bounty-issues-2 · OpencachingDeutschland/oc-	github.com text/html	MISC github.com/OpencachingDeutschland/oc-server3/commit/4bdd6a0e7b7760cea03b91812cbb80d7b16e3b5f

Login required

vuldb.com

text/html

Inactive Link

Not Archived

MISC vuldb.com/?id.215886

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	Opencaching	Oc-server3	-	All	All	All
cpe:2.3:a:opencaching:oc-server3:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @vuldb	[Exploit] Our exploit database now covers CVE-2022-27498, CVE-2022-4514, CVE-2021-4245 and CVE-2022-4511... twitter.com/i/web/status/1...	2022-12-15 12:47:06
 @CVEreport	CVE-2022-4514 : A vulnerability, which was classified as problematic, was found in Opencaching Deutschland oc-serve... twitter.com/i/web/status/1...	2022-12-15 20:09:01
 /r/netcve	CVE-2022-4514	2022-12-15 21:39:46

← 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