

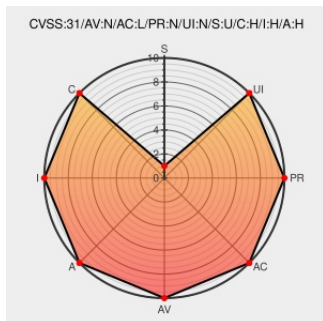


CVE-2021-4295

Published on: Not Yet Published

Last Modified on: 01/06/2023 04:48:00 PM UTC

CVE-2021-4295

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

Certain versions of [Code-validator-api](#) from [Healthit](#) contain the following vulnerability:

A vulnerability classified as problematic was found in ONC code-validator-api up to 1.0.30. This vulnerability affects the function vocabularyValidationConfigurations of the file

src/main/java/org/sitenv/vocabularies/configuration/CodeValidatorApiConfiguration.java of the component XML Handler. The manipulation leads to xml external entity reference. Upgrading to version 1.0.31 is able to address this issue. The name of the patch is fbd8ea121755a2d3d116b13f235bc8b61d8449af. It is recommended to upgrade the affected component. VDB-217018 is the identifier assigned to this vulnerability.

CVE-2021-4295 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVE References

Description	Tags	Link
CVE-2021-4295 ONC code-validator-api XML CodeValidatorApiConfiguration.java vocabularyValidationConfigurations xml external entity reference (ID 97)	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?ctiid.217018
CVE-2021-4295 ONC code-validator-api XML CodeValidatorApiConfiguration.java vocabularyValidationConfigurations xml external	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?id.217018

entity reference (ID 97)

Merge pull request #97 from radiovideo/XXE-vulnerability-fix · onc-healthit/code-validator-api@fbd8ea1 · GitHub

github.com
text/html

MISC github.com/onc-healthit/code-validator-api/commit/fbd8ea121755a2d3d116b13f235bc8b61d8449af

Release SITE 3.1.50 · onc-healthit/code-validator-api · GitHub

github.com
text/html

MISC github.com/onc-healthit/code-validator-api/releases/tag/1.0.31

Fix DocumentBuilderFactory XXE vulnerability by radiovideo · Pull Request #97 · onc-healthit/code-validator-api · GitHub

github.com
text/html

MISC github.com/onc-healthit/code-validator-api/pull/97

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

A vulnerability classified as problematic was found in ONC code-validator-api up to 1.0.30. This vulnerability affect...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Healthit	Code-validator-api	All	All	All	All
cpe:2.3:a:healthit:code-validator-api:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2021-4295	2022-12-29 09:38:19

← 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](#)