



CVE-2022-41255

Published on: Not Yet Published

Last Modified on: 09/22/2022 06:47:00 PM UTC

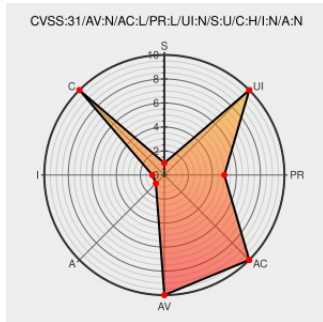
CVE-2022-41255

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Cons3rt](#) from [Jenkins](#) contain the following vulnerability:

Jenkins CONS3RT Plugin 1.0.0 and earlier stores Cons3rt API token unencrypted in job config.xml files on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system.

CVE-2022-41255 has been assigned by jenkinsci-cert@googlegroups.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Jenkins project](#) - [Jenkins CONS3RT Plugin](#) version <= 1.0.0

Affected Vendor/Software: [Jenkins project](#) - [Jenkins CONS3RT Plugin](#) version ?> 1.0.0

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

| Description | Tags | Link |
|--|--|--|
| Jenkins Security Advisory 2022-09-21 | www.jenkins.io text/html | CONFIRM www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2759 |
| oss-security - Multiple vulnerabilities in Jenkins and Jenkins plugins | www.openwall.com text/html | MLIST [oss-security] 20220921 Multiple vulnerabilities in Jenkins and Jenkins plugins |

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.

Related QID Numbers





730618 Jenkins Cross-Site Scripting (XSS) Vulnerability (Jenkins Security Advisory 2022-09-21)

Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|--|---------|---------|---------|--------|---------|----------|
| Application | Jenkins | Cons3rt | All | All | All | All |
| cpe:2.3:a:jenkins:cons3rt:*:*:*:*:jenkins:*:*: | | | | | | |

No vendor comments have been submitted for this CVE

Social Mentions

| Source | Title | Posted (UTC) |
|--|--|---------------------|
|  @CVEreport | CVE-2022-41255 : Jenkins CONS3RT Plugin 1.0.0 and earlier stores Cons3rt API token unencrypted in job config.xml fi... twitter.com/i/web/status/1... | 2022-09-21 16:04:39 |
|  @Inceptus3 | New Vulnerability: CVE-2022-41255 #InceptusSecure #UnderOurProtection | 2022-09-21 18:11:21 |
|  @LinInfoSec | Jenkins - CVE-2022-41255: jenkins.io/security/advis... | 2022-09-21 19:00:37 |
|  /r/netcve | CVE-2022-41255 | 2022-09-21 16:39:12 |

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#)