



Published on: Not Yet Published

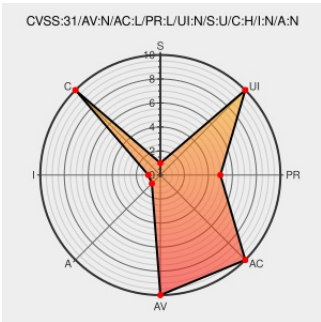
Last Modified on: 02/12/2023 10:10:54 PM UTC

CVE-2022-1632

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

An Improper Certificate Validation attack was found in Openshift. A re-encrypt Route with destinationCACertificate explicitly set to the default serviceCA skips internal Service TLS certificate validation. This flaw allows an attacker to exploit an invalid certificate, resulting in a loss of confidentiality.

CVE-2022-1632 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

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
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/security/cve/cve-2022-1632
2081181 – (CVE-2022-1632) CVE-2022-1632 Openshift: ClusterIP Service TLS certificate not checked by route controller if re-encrypt Route destinationCACertificate field is explicitly set to default serviceCA	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=2081181

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
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Redhat	Ansible Automation Platform	2.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
cpe:2.3:o:fedoraproject:fedora:34:*****::						
cpe:2.3:o:fedoraproject:fedora:35:*****::						
cpe:2.3:a:redhat:ansible_automation_platform:2.0:*****::						
cpe:2.3:a:redhat:openshift_container_platform:4.0:*****::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-1632 : An Improper Certificate Validation attack was found in Openshift. A re-encrypt Route with destinati... twitter.com/i/web/status/1...	2022-09-01 21:05:13

[← 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](#)