



CVE-2021-4294

Published on: Not Yet Published

Last Modified on: 06/26/2023 05:47:00 PM UTC

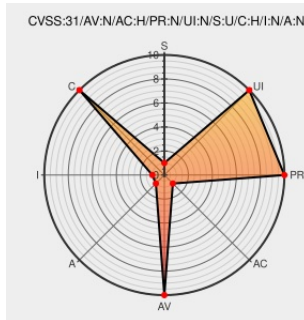
CVE-2021-4294

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [OpenShift Container Platform](#) from [Redhat](#) contain the following vulnerability:

A vulnerability was found in OpenShift OSIN. It has been classified as problematic. This affects the function ClientSecretMatches/CheckClientSecret. The manipulation of the argument secret leads to observable timing discrepancy. The name of the patch is 8612686d6dda34ae9ef6b5a974e4b7accb4fea29. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216987.

CVE-2021-4294 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **OpenShift - OSIN** version = n/a

CVSS3 Score: **5.9 - MEDIUM**

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

CVE References

Description	Tags	Link
Use constant time comparisons for client secrets · openshift/osin@8612686 · GitHub	github.com text/html	MISC github.com/openshift/osin/commit/8612686d6dda34ae9ef6b5a974e4b7accb4fea29
CVE-2021-4294 OpenShift OSIN CheckClientSecret timing discrepancy (ID 200)	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?id.216987

discrepancy (ID 200)

Use constant time
comparisons for client
secrets by stlaz · Pull
Request #200 ·
openshift/osin · GitHub

github.com
text/html

MISC github.com/openshift/osin/pull/200

CVE-2021-4294 |
OpenShift OSIN
CheckClientSecret timing
discrepancy (ID 200)

vuldb.com
text/html

MISC vuldb.com/?ctiid.216987

Inactive Link Not Archived

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 was found in OpenShift OSIN. It has been classified as problematic. This affects the function ClientS...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Osin	1.0.0	All	All	All
Application	Redhat	Openshift Osin	1.0.1	All	All	All
cpe:2.3:a:redhat:openshift_container_platform:4.0:*****:						
cpe:2.3:a:redhat:openshift_osin:1.0.0:*****:						
cpe:2.3:a:redhat:openshift_osin:1.0.1:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-4294 : A vulnerability was found in OpenShift OSIN. It has been classified as problematic. This affects th... twitter.com/i/web/status/1...	2022-12-28 17:07:32
 /r/netcve	CVE-2021-4294	2022-12-28 18:38:20

← 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](#)