



CVE-2020-8551

Published on: 03/27/2020 12:00:00 AM UTC

Last Modified on: 01/27/2023 06:26:00 PM UTC

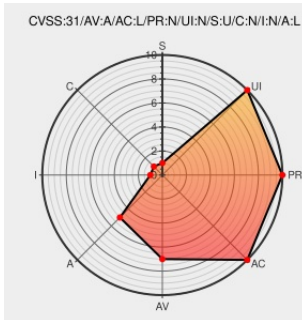
CVE-2020-8551

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The Kubelet component in versions 1.15.0-1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via the kubelet API, including the unauthenticated HTTP read-only API typically served on port 10255, and the authenticated HTTPS API typically served on port 10250.

CVE-2020-8551 has been assigned by security@kubernetes.io to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Kubernetes - Kubernetes** version < v1.17.3

Affected Vendor/Software: **Kubernetes - Kubernetes** version < v1.16.7

Affected Vendor/Software: **Kubernetes - Kubernetes** version < v1.15.10

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Google Groups	Mailing List Third Party Advisory groups.google.com text/html	 MISC groups.google.com/forum/#!topic/kubernetes-security-announce/2UOlSba2g0s
[SECURITY] Fedora 32 Update: origin-3.11.2-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-aeea04cd13
April 2020 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20200413-0003/
CVE-2020-8551: Kubelet DoS via API · Issue #89377 · kubernetes/kubernetes · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/kubernetes/kubernetes/issues/89377

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

[377860](#) Kubernetes kubelet Denial of Service (DoS) Via API Vulnerability

[770020](#) Red Hat OpenShift Container Platform 4.3.10 Security Update (RHSA-2020:1276)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:32:*****:*						
cpe:2.3:a:kubernetes:kubernetes:*****:*						
cpe:2.3:a:kubernetes:kubernetes:*****:*						
cpe:2.3:a:kubernetes:kubernetes:*****:*						

Discovery Credit

Henrik Schmidt

[← 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](#)