

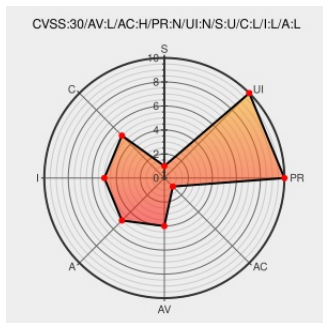


CVE-2019-11245

Published on: 08/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:36 PM UTC

CVE-2019-11245 - advisory for

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

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

In kubelet v1.13.6 and v1.14.2, containers for pods that do not specify an explicit `runAsUser` attempt to run as uid 0 (root) on container restart, or if the image was previously pulled to the node. If the pod specified `mustRunAsNonRoot: true`, the kubelet will refuse to start the container as root. If the pod did not specify `mustRunAsNonRoot: true`, the kubelet will run the container as uid 0.

CVE-2019-11245 has been assigned by [security@kubernetes.io](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Kubernetes](#) - **Kubernetes** version = **v1.13.6**

Affected Vendor/Software: [Kubernetes](#) - **Kubernetes** version = **v1.14.2**

Vulnerability Patch/Work Around

Specify `runAsUser` directives in pods to control the uid a container runs as. Specify `mustRunAsNonRoot:true` directives in pods to prevent starting as root (note this means the attempt to start the container will fail on affected kubelet versions).

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality	Integrity	Availability

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description	Tags	Link
CVE-2019-11245: v1.14.2, v1.13.6: container uid changes to root after first restart or if image is already pulled to the node · Issue #78308 · kubernetes/kubernetes · GitHub	Exploit Patch Third Party Advisory github.com text/html	 CONFIRM github.com/kubernetes/kubernetes/issues/78308
September 2019 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190919-0003/

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

377861 Kubernetes kubelet Container Uid Changes to Root Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Kubernetes	1.13.6	All	All	All
Application	Kubernetes	Kubernetes	1.14.2	All	All	All
Application	Kubernetes	Kubernetes	1.13.6	All	All	All
Application	Kubernetes	Kubernetes	1.14.2	All	All	All

cpe:2.3:a:kubernetes:kubernetes:1.13.6:*:*:*:*:*:

cpe:2.3:a:kubernetes:kubernetes:1.14.2:*:*:*:*:*:

cpe:2.3:a:kubernetes:kubernetes:1.13.6:*:*:*:*:*:

cpe:2.3:a:kubernetes:kubernetes:1.14.2:*:*:*:*:*:

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← 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](#)