



CVE-2019-11246

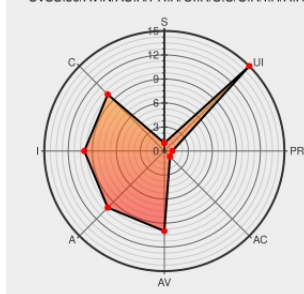
Published on: 08/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:35 PM UTC

CVE-2019-11246 - advisory for

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

CVSS:30/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H



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

The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes runs tar inside the container to create a tar archive, copies it over the network, and kubectl unpacks it on the user's machine. If the tar binary in the container is malicious, it could run any code and output unexpected,

malicious results. An attacker could use this to write files to any path on the user's machine when kubectl cp is called, limited only by the system permissions of the local user. Kubernetes affected versions include versions prior to 1.12.9, versions prior to 1.13.6, versions prior to 1.14.2, and versions 1.1, 1.2, 1.4, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11.

CVE-2019-11246 has been assigned by security@kubernetes.io to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2019-11246: Clean links handling in cp's tar code by soltysh · Pull Request #76788 · kubernetes/kubernetes · GitHub	Patch Third Party Advisory github.com text/html	 CONFIRM github.com/kubernetes/kubernetes/pull/76788
September 2019 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	Third Party Advisory security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190919-0003/
Google Groups	Third Party Advisory groups.google.com text/html	 MLIST [ANNOUNCE] Incomplete fixes for CVE-2019-1002101, kubect! cp potential directory traversal - CVE-2019-11246

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
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.12.11	beta0	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.12.11	beta0	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
cpe:2.3:a:kubernetes:kubernetes:*****.*.*:						
cpe:2.3:a:kubernetes:kubernetes:1.12.11:beta0:*****.*.*:						
cpe:2.3:a:kubernetes:kubernetes:*****.*.*:						
cpe:2.3:a:kubernetes:kubernetes:1.12.11:beta0:*****.*.*:						
cpe:2.3:a:kubernetes:kubernetes:*****.*.*:						

Discovery Credit

Charles Holmes, Atredis Partners

Social Mentions

Source	Title	Posted (UTC)
 /r/TutorialBoy	A Detailed Talk about K8S Cluster Security from the Perspective of Attackers (Part 1)	2022-09-15 17:54:15

© [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](#)