



# CVE-2019-11254

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-11254
<b>State</b>	PUBLIC
<b>Assigner</b>	security@kubernetes.io
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-01 21:15:00 UTC
<b>Updated</b>	2020-10-02 17:37:00 UTC
<b>Description</b>	The Kubernetes API Server component in versions 1.1-1.14, and versions prior to 1.15.10, 1.16.7 and 1.17.3 allows an aut

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Kubernetes</a>	<a href="#">Kubernetes</a>	All	All	All	All
Application	<a href="#">Kubernetes</a>	<a href="#">Kubernetes</a>	All	All	All	All

## References

### Reference

Google Groups

April 2020 Kubernetes Vulnerabilities in NetApp Products | NetApp Product Security

CVE-2019-11254: kube-apiserver Denial of Service vulnerability from malicious YAML payloads · Issue #89535 · kubernetes/kubernetes · GitH

CVE Program record

NVD vulnerability detail

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Mike Danese of Google

## Legacy QID Mappings

[770028](#) Red Hat OpenShift Container Platform 4.5 Security Update (RHSA-2020:2413)

© [CVE.report](#) 2026 |

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](#)