



# CVE-2018-1002105

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-1002105
<b>State</b>	PUBLIC
<b>Assigner</b>	security@kubernetes.io
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-05 21:29:00 UTC
<b>Updated</b>	2023-11-07 02:51:00 UTC
<b>Description</b>	In all Kubernetes versions prior to v1.10.11, v1.11.5, and v1.12.3, incorrect handling of error responses to proxied upgrade

## Risk And Classification

**Problem Types:** CWE-388

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Kubernetes</a>	<a href="#">Kubernetes</a>	1.9.12	beta0	All	All
Application	<a href="#">Kubernetes</a>	<a href="#">Kubernetes</a>	1.9.12	beta0	All	All
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
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
Application	<a href="#">Netapp</a>	<a href="#">Trident</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Trident</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.10	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.11	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.4	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.5	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.6	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.8	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.10	All	All	All

Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.11	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.4	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.5	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.6	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	3.8	All	All	All

## References

### Reference

[Red Hat Customer Portal](#)

[Google Groups](#)

[\[security-announce\] openSUSE-SU-2020:0554-1: important: Security update](#)

[Google Groups](#)

[CVE-2018-1002105 Kubernetes Privilege Escalation Vulnerability in NetApp Products | NetApp Product Security](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Coalfire - Kubernetes Vulnerability: What You Can and Should Do to Protect Your Enterprise](#)

[Kubernetes - \(Unauthenticated\) Arbitrary Requests - Multiple remote Exploit](#)

[Red Hat Customer Portal](#)

[oss-security - Re: linux-distros membership application - Microsoft](#)

[Red Hat Customer Portal](#)

[oss-security - Re: linux-distros membership application - Microsoft](#)

[Kubernetes - \(Authenticated\) Arbitrary Requests - Multiple remote Exploit](#)

[Red Hat Customer Portal](#)

[GitHub - evict/poc\\_CVE-2018-1002105: PoC for CVE-2018-1002105.](#)

[Red Hat Customer Portal](#)

[Kubernetes API Server CVE-2018-1002105 Remote Privilege Escalation Vulnerability](#)

[oss-security - Re: linux-distros membership application - Microsoft](#)

[CVE-2018-1002105: proxy request handling in kube-apiserver can leave vulnerable TCP connections · Issue #71411 · kubernetes/kubernetes](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)