



# CVE-2019-19922

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

## Summary

<b>CVE</b>	CVE-2019-19922
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-22 20:15:00 UTC
<b>Updated</b>	2022-12-14 19:15:00 UTC
<b>Description</b>	kernel/sched/fair.c in the Linux kernel before 5.3.9, when cpu.cfs_quota_us is used (e.g., with Kubernetes), allows attackers

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Aff Baseboard Management Controller</a>	a700	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Data Availability Services</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">E-series Santricity Os Controller</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Fas/aff Baseboard Management Controller</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Baseboard Management Controller</a>	h610s	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Steelstore Cloud Integrated Storage</a>	-	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Sd-wan Edge</a>	8.2	All	All	All

## References

Reference	Source	Link
CFS quotas can lead to unnecessary throttling · Issue #67577 · kubernetes/kubernetes · GitHub	MISC	<a href="#">github.com</a>
January 2020 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
USN-4226-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>
sched/fair: Fix low cpu usage with high throttling by removing expira... · torvalds/linux@de53fd7 · GitHub	MISC	<a href="#">github.com</a>
<a href="#">cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.9</a>	MISC	<a href="#">cdn.kernel.org</a>
[SECURITY] [DLA 2068-1] linux security update	MLIST	<a href="#">lists.debian.org</a>
<a href="#">kernel/git/torvalds/linux.git</a> - Linux kernel source tree	MISC	<a href="#">git.kernel.org</a>
The Kernel Change That May Be Slowing Down Your App – Repeatable Systems	MISC	<a href="#">relistan.com</a>
Oracle Critical Patch Update Advisory - April 2021	MISC	<a href="#">www.oracle.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

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](#)