



# CVE-2022-34494

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

## Summary

<b>CVE</b>	CVE-2022-34494
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-26 16:15:00 UTC
<b>Updated</b>	2022-07-08 03:59:00 UTC
<b>Description</b>	rpmsg_virtio_add_ctrl_dev in drivers/rpmsg/virtio_rpmsg_bus.c in the Linux kernel before 5.18.4 has a double free.

## Risk And Classification

**Problem Types:** CWE-415

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

## References

Reference	Source	Link	Tags
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.18.4	MISC	<a href="https://cdn.kernel.org">cdn.kernel.org</a>	
rpmsg: virtio: Fix possible double free in rpmsg_virtio_add_ctrl_dev() · torvalds/linux@1680939 · GitHub	MISC	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 183701 Debian Security Update for linux (CVE-2022-34494)
- 198860 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5517-1)
- 198868 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5529-1)
- 198948 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5624-1)

198950 Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-5623-1)
198953 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5633-1)
198958 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5635-1)
198960 Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-5640-1)
198964 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5644-1)
198967 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5648-1)
198972 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5655-1)
198989 Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5683-1)
354018 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-003
354022 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-002
354024 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-004
354270 Amazon Linux Security Advisory for kernel : ALAS2022-2022-114
354468 Amazon Linux Security Advisory for kernel : ALAS2022-2022-185
354542 Amazon Linux Security Advisory for kernel : ALAS-2022-185
355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
610451 Google Pixel Android December 2022 Security Patch Missing
6140253 AWS Bottlerocket Security Update for kernel (GHSA-wrfg-8xmp-r9wp)
902408 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9995)
902412 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9986)
902617 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9986-1)
902676 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9995-1)
906146 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9995-2)
906347 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9986-2)

© [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](#)