



# CVE-2019-19063

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

## Summary

<b>CVE</b>	CVE-2019-19063
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-11-18 06:15:00 UTC
<b>Updated</b>	2023-11-07 03:07:00 UTC
<b>Description</b>	Two memory leaks in the rtl_usb_probe() function in drivers/net/wireless/realtek/rtlwifi/usb.c in the Linux kernel through 5.3.

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Broadcom	Brocade Fabric Operating System Firmware	-	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Aff Baseboard Management Controller	-	All	All	All

Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Data Availability Services	-	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.0	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.0.0	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.20	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.25	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.30	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.30.5r3	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.40	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.40.3r2	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.40.5	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.50.1	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.50.2	-	All	All
Application	Netapp	E-series Santricity Os Controller	11.50.2	p1	All	All
Application	Netapp	E-series Santricity Os Controller	11.60	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.60.0	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.60.1	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.60.3	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.70.1	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.70.2	All	All	All
Application	Netapp	Fas/aff Baseboard Management Controller	-	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h610s	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Operating System	Netapp	Hci Compute Node Firmware	-	All	All	All
Application	Netapp	Solidfire Enterprise Sds Hci Storage Node	-	All	All	All
Hardware	Netapp	Solidfire Baseboard Management Controller	-	All	All	All
Operating System	Netapp	Solidfire Baseboard Management Controller Firmware	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Oracle	Sd-wan Edge	8.2	All	All	All

## References

Reference	Source	Link
-----------	--------	------

Microsoft, 2016. Microsoft Windows Server 2016 Datacenter. Microsoft. CONFIDENTIAL

November 2019 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2020-008-01)	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>
USN-4284-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[SECURITY] Fedora 31 Update: kernel-5.3.12-300.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
USN-4287-2: Linux kernel (Azure) vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[SECURITY] Fedora 30 Update: kernel-5.3.12-200.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
USN-4254-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
USN-4285-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[security-announce] openSUSE-SU-2019:2675-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
USN-4254-2: Linux kernel (Xenial HWE) vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
rtlwifi: prevent memory leak in rtl_usb_probe · torvalds/linux@3f93616 · GitHub	MISC	<a href="https://github.com">github.com</a>
Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>
USN-4287-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
[SECURITY] Fedora 30 Update: kernel-5.3.12-200.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 31 Update: kernel-5.3.12-300.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Oracle Critical Patch Update Advisory - April 2021	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159420](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9473)

[159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)

[390248](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0035)

[940256](#) AlmaLinux Security Update for kernel (ALSA-2020:4431)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)