



CVE-2019-16232

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

Summary

CVE	CVE-2019-16232
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-11 16:15:00 UTC
Updated	2023-11-07 03:05:00 UTC
Description	drivers/net/wireless/marvell/libertas/if_sdio.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, le

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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	5.2.14	All	All	All
Operating System	Linux	Linux Kernel	5.2.14	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All

Operating System	Opensuse	Leap	15.1	All	All	All
------------------	--------------------------	----------------------	------	-----	-----	-----

References

Reference	Source	Link	Ta
[SECURITY] Fedora 30 Update: kernel-5.3.14-200.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
September 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Th
[SECURITY] Fedora 31 Update: kernel-5.3.14-300.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Ma
[security-announce] openSUSE-SU-2019:2392-1: important: Security update	SUSE	lists.opensuse.org	Ma
USN-4284-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Th
USN-4287-2: Linux kernel (Azure) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Th
USN-4285-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Th
USN-4287-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Th
LKML: Semmlé Security Reports: Multiple NULL deref on alloc_workqueue	MISC	lkml.org	Ex
[SECURITY] Fedora 30 Update: kernel-5.3.14-200.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Ma
[SECURITY] Fedora 31 Update: kernel-5.3.14-300.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[security-announce] openSUSE-SU-2019:2444-1: important: Security update	SUSE	lists.opensuse.org	Ma
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[198323](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4904-1)

© [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