



# CVE-2019-3701

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

## Summary

<b>CVE</b>	CVE-2019-3701
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-01-03 16:29:00 UTC
<b>Updated</b>	2019-09-03 00:15:00 UTC
<b>Description</b>	An issue was discovered in can_can_gw_rcv in net/can/gw.c in the Linux kernel through 4.19.13. The CAN frame modification

## Risk And Classification

**Problem Types:** CWE-787

## 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>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	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

## References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:0543-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>	
kernel/git/netdev/net.git - Netdev Group's networking tree	MISC	<a href="#">git.kernel.org</a>	Mailing List, Pa
support.f5.com/csp/article/K17957133	CONFIRM	<a href="#">support.f5.com</a>	Third Party Ad
USN-3932-2: Linux kernel (Xenial HWE) vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubuntu.com</a>	Third Party Ad
[SECURITY] [DLA 1731-2] linux regression update	MLIST	<a href="#">lists.debian.org</a>	Mailing List, Tr
[SECURITY] [DLA 1771-1] linux-4.9 security update	MLIST	<a href="#">lists.debian.org</a>	Mailing List, Tr
USN-3932-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubuntu.com</a>	Third Party Ad

USN-4118-1: Linux kernel (AWS) vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
'[PATCH v3] can: gw: ensure DLC boundaries after CAN frame modification' - MARC	MISC	<a href="https://marc.info">marc.info</a>	Mailing List, Pa
Linux Kernel 'can_can_gw_rcv in net/can/gw.c' Local Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Ad
[SECURITY] [DLA 1731-1] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Mailing List, Th
'[PATCH] can: gw: ensure DLC boundaries after CAN frame modification' - MARC	MISC	<a href="https://marc.info">marc.info</a>	Patch, Third Pa
USN-4115-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
Bug 1120386 – VUL-0: CVE-2019-3701: kernel: crash in CAN driver	MISC	<a href="https://bugzilla.suse.com">bugzilla.suse.com</a>	Exploit, Issue T
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, ana

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[750691](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1141-1)

© [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](#).

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