



# CVE-2019-3459

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

## Summary

<b>CVE</b>	CVE-2019-3459
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-11 16:29:00 UTC
<b>Updated</b>	2023-11-07 03:09:00 UTC
<b>Description</b>	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1.

## Risk And Classification

### Problem Types: CWE-125

## 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>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	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="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	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
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	5.0	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time</a>	7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time</a>	8	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time For Nfv</a>	7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time For Nfv</a>	8	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time For Nfv Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time For Nfv Tus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time Tus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Mrg</a>	2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Mrg</a>	2.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Enterprise Mrg</a>	2.0	All	All	All

## References

Reference	Source	Li
Red Hat Customer Portal	REDHAT	ac
oss-security - Re: linux-distros membership application - Microsoft	MLIST	wv
[SECURITY] [DLA 1799-2] linux security update	MLIST	lis
oss-security - Re: linux-distros membership application - Microsoft	MLIST	wv
Red Hat Customer Portal	REDHAT	ac
oss-security - Re: linux-distros membership application - Microsoft	MLIST	wv
[SECURITY] [DLA 1799-1] linux security update	MLIST	lis
Red Hat Customer Portal	REDHAT	ac
[PATCH 1/2] Bluetooth: check message types in l2cap_get_conf_opt - Greg Kroah-Hartman	MLIST	lor
Red Hat Customer Portal	REDHAT	ac

[oss-security] Linux kernel: Bluetooth: two remote intoleaks (CVE-2019-3459, CVE-2019-3460) - MAHC	MLIST	ml
Red Hat Customer Portal	REDHAT	ac
Access Denied	CONFIRM	bu
[SECURITY] [DLA 1771-1] linux-4.9 security update	MLIST	lis
CVE-2019-3459   Ubuntu	CONFIRM	pe
oss-security - Re: linux-distros membership application - Microsoft	MLIST	wv
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git
oss-security - Re: linux-distros membership application - Microsoft	MLIST	wv
1663176 – (CVE-2019-3459) CVE-2019-3459 kernel: Heap address information leak while using L2CAP_GET_CONF_OPT	CONFIRM	bu
[PATCH 1/2] Bluetooth: check message types in l2cap_get_conf_opt - Greg Kroah-Hartman		lo
Red Hat Customer Portal	REDHAT	ac
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**