



CVE-2019-3460

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

Summary

CVE	CVE-2019-3460
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-11 16:29:00 UTC
Updated	2023-11-07 03:09:00 UTC
Description	A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-r

Risk And Classification

Problem Types: CWE-20


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	18.10	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	18.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Redhat	Codeready Linux Builder	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All

Operating System	Redhat	Enterprise Linux For Real Time	7	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time	8	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv	7	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv	8	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux For Real Time Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference	Source
Red Hat Customer Portal	REDHAT
oss-security - Re: linux-distros membership application - Microsoft	MLIST
[SECURITY] [DLA 1799-2] linux security update	MLIST
oss-security - Re: linux-distros membership application - Microsoft	MLIST
Red Hat Customer Portal	REDHAT
oss-security - Re: linux-distros membership application - Microsoft	MLIST
[SECURITY] [DLA 1799-1] linux security update	MLIST
Red Hat Customer Portal	REDHAT
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM
'[oss-security] Linux kernel: Bluetooth: two remote infoleaks (CVE-2019-3459, CVE-2019-3460)' - MARC	MLIST
Red Hat Customer Portal	REDHAT
[SECURITY] [DLA 1771-1] linux-4.9 security update	MLIST
1663179 – (CVE-2019-3460) CVE-2019-3460 kernel: Heap address information leak while using L2CAP_PARSE_CONF_RSP	CONFIRM
[PATCH 2/2] Bluetooth: check the buffer size for some messages before parsing - Greg Kroah-Hartman	MLIST
oss-security - Re: linux-distros membership application - Microsoft	MLIST
oss-security - Re: linux-distros membership application - Microsoft	MLIST
Red Hat Customer Portal	REDHAT
CVE-2019-3460	CONFIRM

CVE-2019-3460 in Ubuntu	CONFIRM
[PATCH 2/2] Bluetooth: check the buffer size for some messages before parsing - Greg Kroah-Hartman	
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
	
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](#)