CVE-2019-3459

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-3459
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 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	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	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All

Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	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	Enterprise Mrg	2.0	All	All	All
Operating System	Redhat	Enterprise Mrg	2.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All

References

Reference	Source	Li
Red Hat Customer Portal	REDHAT	ac
oss-security - Re: linux-distros membership application - Microsoft	MLIST	ww
[SECURITY] [DLA 1799-2] linux security update	MLIST	lis
oss-security - Re: linux-distros membership application - Microsoft	MLIST	ww
Red Hat Customer Portal	REDHAT	ac
oss-security - Re: linux-distros membership application - Microsoft	MLIST	ww
[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

'[oss-security] Linux kernel: Bluetooth: two remote infoleaks (CVE-2019-3459, CVE-2019-3460)' - MARC	MLIST	ma
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	ww
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git
oss-security - Re: linux-distros membership application - Microsoft	MLIST	ww
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		lor
Red Hat Customer Portal	REDHAT	ac
CVE Program record	CVE.ORG	ww
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.