



CVE-2019-15917

Published on: 09/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

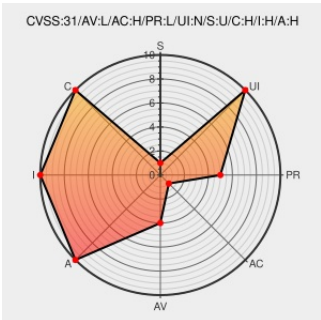
CVE-2019-15917

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

An issue was discovered in the Linux kernel before 5.0.5. There is a use-after-free issue when `hci_uart_register_dev()` fails in `hci_uart_set_proto()` in `drivers/bluetooth/hci_ldisc.c`.

CVE-2019-15917 has been assigned by [M](#) `cve@mitre.org` to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2020-008-01)	Mailing List Third Party Advisory seclists.org text/html	BUGTRAQ 20200109 [slackware-security] Slackware 14.2 kernel (SSA:2020-008-01)

September 2019 Linux
Kernel Vulnerabilities in
NetApp Products | NetApp
Product Security

Third Party Advisory
security.netapp.com
text/html

CONFIRM security.netapp.com/advisory/ntap-20191004-0001/

[SECURITY] [DLA 1930-1]
linux security update

Third Party Advisory
lists.debian.org
text/html

MLIST [debian-lts-announce] 20190925 [SECURITY] [DLA 1930-1] linux security update

[security-announce]
openSUSE-SU-2019:2181-1:
important: Security update

Third Party Advisory
lists.opensuse.org
text/html

SUSE openSUSE-SU-2019:2181

[SECURITY] [DLA 2114-1]
linux-4.9 security update

Third Party Advisory
lists.debian.org
text/html

MLIST [debian-lts-announce] 20200302 [SECURITY] [DLA 2114-1] linux-4.9 security update

Release Notes
cdn.kernel.org
text/plain

MISC cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.0.5

[security-announce]
openSUSE-SU-2019:2173-1:
important: Security update

Third Party Advisory
lists.opensuse.org
text/html

SUSE openSUSE-SU-2019:2173

Slackware Security Advisory
- Slackware 14.2 kernel
Updates ≈ Packet Storm

Third Party Advisory
VDB Entry
packetstormsecurity.com
text/html

MISC packetstormsecurity.com/files/155890/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html

Bluetooth: hci_ldisc:
Postpone
HCI_UART_PROTO_READY
bit set in hci_ua...
torvalds/linux@56897b2 ·
GitHub

Patch
github.com
text/html

MISC
github.com/torvalds/linux/commit/56897b217a1d0a91c9920cb418d6b3fe922f590a

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

159684 Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)

940256 AlmaLinux Security Update for kernel (ALSA-2020:4431)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
Operating System	Linux	Linux Kernel	All	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
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#)