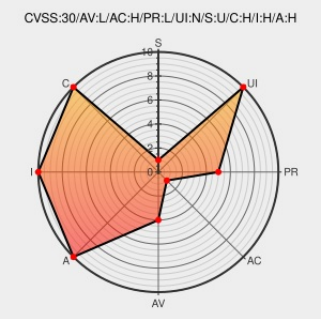
CVE-2018-5814

Published on: 06/12/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5814

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

In the Linux Kernel before version 4.16.11, 4.14.43, 4.9.102, and 4.4.133, multiple race condition errors when handling probe, disconnect, and rebind operations can be exploited to trigger a use-after-free condition or a NULL pointer dereference by sending multiple USB over IP packets.

CVE-2018-5814 has been assigned by PSIRT-CNA@flexerasoftware.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Linux Foundation** - **Linux Kernel** version **Before version 4.16.11, 4.14.43, 4.9.102, and 4.4.133**

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

[security-announce] openSUSE-SU-2019:1407-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2019:1407
USN-3696-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3696-2
USN-3752-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3752-1
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.133
USN-3752-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3752-2
USN-3696-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3696-1
[SECURITY] [DLA 1422-1] linux security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180714 [SECURITY] [DLA 1422-1] linux security update
Linux Kernel USB Over IP Processing Bugs Lets Remote Users Deny Service - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041050
[SECURITY] [DLA 1423-1] linux-4.9 new package	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180718 [SECURITY] [DLA 1423-1] linux-4.9 new package
[SECURITY] [DLA 1422-2] linux security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180715 [SECURITY] [DLA 1422-2] linux security update
kernel/git/stable/linux.git - Linux kernel stable tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=22076557b07c12086eeb16b8ce2b0b735f7a27e7
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.102
Security Advisory SA81540 - Linux Kernel USB over IP Multiple Denial of Service Vulnerabilities - Secunia	Third Party Advisory secuniaresearch.flexerasoftware.com text/html	SECUNIA 81540
USN-3752-3: Linux kernel (Azure, GCP, OEM) vulnerabilities | Ubuntu security notices | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3752-3
Secunia Advisories	Third Party Advisory secuniaresearch.flexerasoftware.com text/html	MISC secuniaresearch.flexerasoftware.com/secunia_research/2018-8/
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.16.11
	Vendor Advisory cdn.kernel.org	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.14.43

	text/plain	
kernel/git/stable/linux.git - Linux kernel stable tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=c171654caa875919be3c533d3518da8be5be966e

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

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:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→