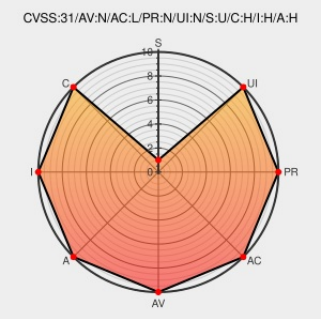
CVE-2018-20961

Published on: 08/07/2019 12:00:00 AM UTC

Last Modified on: 01/19/2023 04:14:00 PM UTC

CVE-2018-20961

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



Certain versions of Linux Kernel from Linux contain the following vulnerability:

In the Linux kernel before 4.16.4, a double free vulnerability in the f_midi_set_alt function of drivers/usb/gadget/function/f_midi.c in the f_midi driver may allow attackers to cause a denial of service or possibly have unspecified other impact.

CVE-2018-20961 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
	Release Notes Vendor Advisory cdn.kernel.org text/plain	MISC cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.16.4

No Description Provided	support.f5.com text/html	CONFIRM support.f5.com/csp/article/K58502654
No Description Provided	support.f5.com text/html	CONFIRM support.f5.com/csp/article/K58502654?utm_source=f5support&utm_medium=RSS
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-238-01)	seclists.org text/html	BUGTRAQ 20190826 [slackware-security] Slackware 14.2 kernel (SSA:2019-238-01)
USB: gadget: f_midi: fixing a possible double-free in f_midi · torvalds/linux@7fafcfd · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/7fafcfdf6377b18b2a726ea554d6e593ba44349f
Kernel Live Patch Security Notice LSN-0058-1 ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/154951/Kernel-Live-Patch-Security-Notice-LSN-0058-1.html
Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/154228/Slackware-Security-Advisory-Slackware-14.2-kernel-Updates.html
August 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20190905-0002/
kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit Mailing List Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=7fafcfdf6377b18b2a726ea554d6e593ba44349f
USN-4145-1: Linux kernel vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-4145-1

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

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→