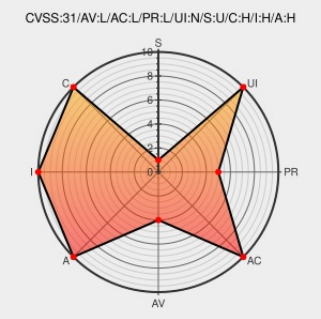
CVE-2022-3170

Published on: Not Yet Published

Last Modified on: 12/08/2022 10:06:00 PM UTC

CVE-2022-3170

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



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

An out-of-bounds access issue was found in the Linux kernel sound subsystem. It could occur when the 'id->name' provided by the user did not end with '\0'. A privileged local user could pass a specially crafted name through ioctl() interface and crash the system or potentially escalate their privileges on the system.

CVE-2022-3170 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
ALSA: control: Re-order bounds checking in get_ctl_id_hash() · torvalds/linux@5934d9a · GitHub	github.com text/html	MISC github.com/torvalds/linux/commit/5934d9a0383619c14df91af8fd76261dc3de2f5f
ALSA: control: Fix an out-of-bounds bug in get_ctl_id_hash() · torvalds/linux@6ab55ec · GitHub	github.com text/html	MISC github.com/torvalds/linux/commit/6ab55ec0a938c7f943a4edba3d6514f775983887

Related QID Numbers

903910 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10948)

903942 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10924)

904107 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10948-1)

904246 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10924-1)

905752 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10948-2)

906433 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10924-2)

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	6.0	rc1	All	All
Operating System	Linux	Linux Kernel	6.0	rc2	All	All
Operating System	Linux	Linux Kernel	6.0	rc3	All	All

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

cpe:2.3:o:linux:linux_kernel:6.0:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.0:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:6.0:rc3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-3170 : An out-of-bounds access issue was found in the #Linux #kernel sound subsystem. It could occur when… twitter.com/i/web/status/1…	2022-09-13 16:06:11
/r/netcve	CVE-2022-3170	2022-09-13 16:38:28

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report