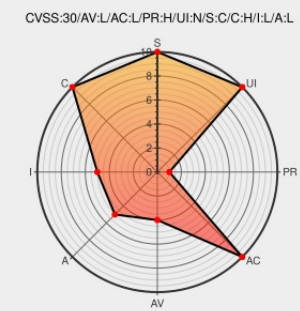
CVE-2022-2652

Published on: Not Yet Published

Last Modified on: 08/10/2022 01:40:00 PM UTC

CVE-2022-2652 - advisory for 1b055da5-7a9e-4409-99d7-030280d242d5

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



Certain versions of V4l2loopback from V4l2loopback Project contain the following vulnerability:

Depending on the way the format strings in the card label are crafted it's possible to leak kernel stack memory. There is also the possibility for DoS due to the v4l2loopback kernel module crashing when providing the card label on request (reproduce e.g. with many %s modifiers in a row).

CVE-2022-2652 has been assigned by security@huntr.dev to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **umlaeute** - **umlaeute/v4l2loopback** version **< 0.12.6**

CVSS3 Score: 6 - MEDIUM

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

CVE References

Description	Tags	Link
add explicit format specifier to printf() invocations · umlaeute/v4l2loopback@e4cd225 · GitHub	github.com text/html	MISC github.com/umlaeute/v4l2loopback/commit/e4cd225557486c420f6a34411f98
huntr – Security Bounties for any GitHub repository	huntr.dev text/html Inactive Link Not Archived	CONFIRM huntr.dev/bounties/1b055da5-7a9e-4409-99d7-030280d242d5

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

183507 Debian Security Update for v4l2loopback (CVE-2022-2652)

752692 OpenSUSE Security Update for v4l2loopback (openSUSE-SU-2022:10160-1)

752693 OpenSUSE Security Update for v4l2loopback (openSUSE-SU-2022:10159-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	V4l2loopback Project	V4l2loopback	All	All	All	All

cpe:2.3:o:v4l2loopback_project:v4l2loopback:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@AVGFree	@_danielberanek SentinelOne nám dne 20. prosince 2021 nahlásil dvě zranitelnosti, nyní sledované jako CVE-2022-2652… twitter.com/i/web/status/1…	2022-05-10 08:32:31
@vigilance_en	Vigil@nce #Vulnerability of pgjdbc: file write via FileHandler. vigilance.fr/vulnerability/… Identifiers: #CVE-2022-2652… twitter.com/i/web/status/1…	2022-08-01 06:09:04
@CVEreport	CVE-2022-2652 : Depending on the way the format strings in the card label are crafted it's possible to leak #kernel… twitter.com/i/web/status/1…	2022-08-04 09:48:34
@threatmeter	CVE-2022-2652 Depending on the way the format strings in the card label are crafted it's possible to leak kernel st… twitter.com/i/web/status/1…	2022-08-05 07:09:46
@OpenSourceHacks	(CVE-2022-2652): Use of Externally-Controlled Format String in umlaeute/v4l2loopback. huntr.dev/bounties/1b055… Dis… twitter.com/i/web/status/1…	2022-08-07 09:34:45
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-2652 - Depending on the way the format strings in the card label are crafted… twitter.com/i/web/status/1…	2022-08-10 13:42:16
/r/netcve	CVE-2022-2652	2022-08-04 10:38:13

← Previous ID

Next ID→