Format string modifiers in card label in umlaeute/v4l2loopback

1

Valid Reported on Jul 28th 2022

Description

When adding a new video device with `v4l2loopback-ctl` that contains a card label with format string modifiers the kernel driver interprets these when querying the device capabilities, thus leaking kernel memory (stack contents).
The vulnerability requires the attacker to have access to the `/dev/v4l2loopback`, which is owned by `root:root` with `chmod 600` by default. This attack can still be used successfully against kernels in lock down mode.

Proof of Concept

```
v4l2loopback-ctl add -n "%p-%p-%p"
cat /sys/devices/virtual/video4linux/video2/name
```

Output (example):

```
/dev/video2
00000000de899e9f-00000000f6d35a
```

Expected:

```
/dev/video2
%p-%p-%p
```

Impact

Depending on the way the format strings in the card label are crafted it's po
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).

Occurrences

C v4l2loopback.c L2497

The third argument to `snprintf` should be a constant `"%s"` instead of user-controlled.

C v4l2loopback.c L759

The third argument to `snprintf` should be a constant `"%s"` instead of user-controlled.

References

- Casual C Code Reviewers (C3Review)

CVE
CVE-2022-2652
(Published)

Vulnerability Type
CWE-134: Use of Externally-Controlled Format String

Severity
High (7.3)

Registry
Other

Affected Version
0.12.5

Visibility
Public

Status
Fixed

Found by

benbe
@benbe

unranked

Fixed by

benbe

@benbe

unranked

This report was seen 443 times.

We are processing your report and will contact the **umlaeute/v4l2loopback** team within 24 hours. 4 months ago

benbe submitted a **patch** 4 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 4 months ago

umläute modified the Severity from High (8.1) to High (7.3) 4 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

umläute validated this vulnerability 4 months ago

benbe has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

umläute marked this as fixed in **0.12.6** with commit **e4cd22** 4 months ago

benbe has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

v4l2loopback.c#L759 has been validated ✓

v4l2loopback.c#L2497 has been validated ✓

Sign in to join this conversation