

 camelot-os / **sentry-kernel** Public[Code](#) [Issues](#) 17 [Pull requests](#) 10 [Actions](#) [Projects](#) [Wiki](#) [Security](#)

# Incomplete ownership check for IRQ line manipulation

Moderate PThierry published [GHSA-5hgv-rg2f-79pg](#) last week

## Package

No package listed

## Affected versions

< 0.4.7

## Patched versions

0.4.7

## Description

### Impact

A given task with one of the DEV or IO capability is able to interact with another task's IRQ line through the `_sys_int*` syscall family. This can lead to DoS and covert-channels between this task and the outer world.

### Patches

The patch has been delivered in the pull request [#108](#).

### Workarounds

If using releases before v0.4.7, reduce tasks that having the DEV and IO capability to a single one.

### References

Explanation and fix is defined in the corresponding PR:

[#108](#)

## Severity

Moderate

5.1 / 10

### CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	High

[Learn more about base metrics](#)

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H

### CVE ID

CVE-2026-40337

### Weaknesses

► CWE-283

### Credits



PThierry

Remediation developer