net: ip/tcp: Null pointer dereference can be triggered by a race condition

Moderate **ceolin** published **GHSA-4vqm-pw24-g9jp** 50 minutes ago

Package

zephyr (zephyr)

Affected versions

<= 4.3

Patched versions

None

Description

The `tcp_recv()` function in `subsys/net/ip/tcp.c` contains a null pointer dereference vulnerability that can be triggered by a race condition:

Details

1. The protocol stack releases a TCP connection via `tcp_conn_release()`, which sets `conn->context->tcp = NULL` at line 881, and later removes the connection while holding `tcp_lock` (lines 911–913).
2. Meanwhile, packets that have just been received for that same connection may still be processed by `tcp_recv()`. The function first attempts to obtain an existing connection by calling `tcp_conn_search()` (line 2308), which is also protected by `tcp_lock`. If the removal in step 1 happens first, `tcp_conn_search()` returns NULL. If the packet is a SYN, the operation at line 2316 can then result in a null pointer, because `user_data` points to `conn->context` (as set in `zsock_listen_ctx()`). This null pointer is subsequently dereferenced by `tcp_backlog_is_full()` without a prior check.

Patches

main: #102110

For more information

If you have any questions or comments about this advisory:

- Open an issue in zephyr
- Email us at Zephyr-vulnerabilities
  embargo: 2026-03-20

Severity

Moderate 6.4 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-5590

Weaknesses

▶ CWE-476