Out-of-Bounds Write via Unsanitized Prefix Length in Router Advertisement Processing in FreeRTOS-Plus-TCP

High **AniruddhaKanhere** published **GHSA-97qg-4359-xm3x** 3 hours ago

Package

No package listed

Affected versions

>=V4.0.0 AND <=V4.2.5, >=V4.3.0 AND <=V4.4.0

Patched versions

V4.2.6, V4.4.1

Description

Summary

FreeRTOS-Plus-TCP is an open source TCP/IP stack implementation specifically designed for FreeRTOS. The stack provides a standard Berkeley sockets interface and supports essential networking protocols including IPv6, ARP, DHCP, DNS, LLMNR, mDNS, NBNS, RA, ND, ICMP, and ICMPv6.

A bounds-write issue exists in FreeRTOS-Plus-TCP's IPV6 Router Advertisement (RA) packet processing, where an incorrect length value can cause the system to write beyond the allocated memory buffer.

Impact

In the FreeRTOS-Plus-TCP IPV6 Router Advertisement processing which may allow an unauthenticated adjacent-network actor to compromise devices via rogue RA packet.

A section of Router Advertisement processing lacks sufficient validation of length fields during packet parsing, allowing their use in memory operations without proper bounds checking. This can lead to out-of-bounds memory writes. The issue can be exploited by any device on the local network that can send crafted Router Advertisement packets.

New version V4.2.6 and V4.4.1 adds additional input validation to the RA option parser to reject malformed values before they reach sensitive operations.

Any device using FreeRTOS-Plus-TCP versions between V4.0.0 through V4.2.5 and V4.3.0 through V4.4.0, processing Router Advertisement packets is affected by this risk. Update to version V4.4.1 and V4.2.6 or later to fix this.

Patches

This issue has been addressed in FreeRTOS-Plus-TCP version V4.4.1 and V4.2.6. We recommend upgrading to the latest version and ensuring any forked or derivative code is patched to incorporate the new fixes.

Workarounds

- Implement network-level filtering to block untrusted Router Advertisement packets on the local network segment.
- Deploy devices on isolated network segments where rogue RA packets cannot be injected.

References

If you have any questions or comments about this advisory, we ask that you contact AWS Security via our issue reporting page or directly via email to aws-security@amazon.com. Please do not create a public GitHub issue.

Acknowledgement

We would like to thank **@Eun0us** from Espilon for collaborating on this issue through the coordinated issue disclosure process.

Severity

High 8.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-7426

Weaknesses

No CWEs