



## Issue with FreeRTOS-Plus-TCP - IPv6 Router Advertisement Memory Safety Issues

**Bulletin ID:** 2026-023-AWS

**Scope:** AWS

**Content Type:** Important (requires attention)

**Publication Date:** 04/29/2026 11:45 AM PDT

### Description:

FreeRTOS-Plus-TCP is an open source TCP/IP stack implementation designed for FreeRTOS, providing a standard Berkeley sockets interface and support for essential networking protocols including IPv6, ARP, DHCP, DNS, and Router Advertisement (RA). We identified [CVE-2026-7425](#) and [CVE-2026-7426](#), one of them being out-of-bounds read and another one being out-of-bounds write issues respectively in the IPv6 Router Advertisement option parser where insufficient validation of length fields allows memory operations without proper bounds checking.

Either issue can be exploited by any device on the local network that can send crafted Router Advertisement packets. No authentication or user interaction is required.



**Impacted versions:**  $\geq V4.0.0$  AND  $\leq V4.2.5$ ,  $\geq V4.3.0$  AND  $\leq V4.4.0$

### Resolution:

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:

If upgrading is not immediately possible, consider the following mitigations:

- 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:

- [CVE-2026-7425](#)
- [CVE-2026-7426](#)
- [GHSA-gffr-xqjg-jh9j](#)
- [GHSA-97qg-4359-xm3x](#)

### Acknowledgment:

We would like to thank Espilon for collaborating on this issue through the coordinated vulnerability disclosure process.

Please email [aws-security@amazon.com](mailto:aws-security@amazon.com) with any security questions or concerns.



