CVE-2026-7424 - Integer Underflow in DHCPv6 Sub-Option Parser in FreeRTOS-Plus-TCP

Bulletin ID: 2026-022-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, scalable TCP/IP stack for FreeRTOS. We identified CVE-2026-7424, where an integer underflow issue in the DHCPv6 sub-option parser could allow an adjacent network user to corrupt the device's IPv6 address assignment, DNS configuration, and lease times, and to cause a denial of service (IP task freeze requiring hardware reset).

Impacted versions: FreeRTOS-Plus-TCP >=V4.0.0 AND <=V4.2.5, >=V4.3.0 AND <= 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:

Users who cannot immediately upgrade can disable DHCPv6 by setting ipconfigUSE_DHCPv6 to 0 in their FreeRTOSIPConfig.h configuration file. Note that this workaround requires manual IPv6 address configuration.

References:

- CVE-2026-7424
- GHSA-wrhm-c99p-2p8g

Acknowledgment:

We would like to thank security researcher @Eun0us | Espilon for collaborating on this issue through the coordinated vulnerability disclosure process.

Please email aws-security@amazon.com with any security questions or concerns.