Integer Underflow in DHCPv6 Sub-Option Parser in FreeRTOS-Plus-TCP

High **AniruddhaKanhere** published **GHSA-wrhm-c99p-2p8g** 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 a lightweight TCP/IP stack for FreeRTOS. An issue exists where, under certain circumstances, a crafted DHCPv6 message can cause integer underflow in the sub-option parser, leading to parser state corruption and denial of service.

Impact

Integer underflow in the DHCPv6 sub-option parser in FreeRTOS-Plus-TCP before V4.4.1/V4.2.6 allows an adjacent network actor to corrupt the device's IPv6 address assignment, DNS configuration, and lease times, and to cause a denial of service (permanent IP task freeze requiring hardware reset) by sending a single crafted DHCPv6 packet.

Impacted versions: >=V4.0.0 AND <=V4.2.5, >=V4.3.0 AND <=V4.4.0

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

Disable DHCPv6 if IPv6 address assignment can be configured statically. Alternatively, implement network-level filtering to restrict DHCPv6 traffic to trusted sources on the local network segment.

References

If you have any questions or comments about this advisory, we ask that you contact AWS Security via our vulnerability 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 security researcher **@Eun0us** | Espilon for collaborating on this issue through the coordinated vulnerability 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-2026-7424

Weaknesses

No CWEs