Out-of-Bounds Read in Router Advertisement Option Parser in FreeRTOS-Plus-TCP

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-7425
State	PUBLISHED
Assigner	AMZN
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-29 20:16:32 UTC
Updated	2026-04-29 23:16:20 UTC
Description	Insufficient option length validation in the IPv6 Router Advertisement parser in FreeRTOS-Plus-TCP before V4.2.6 and V4.4

Risk And Classification

Primary CVSS: v4.0 6 MEDIUM from ff89ba41-3aa1-4d27-914a-91399e9639e5

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-125 | CWE-125 CWE-125: Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	6	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	6	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:
3.1	ff89ba41-3aa1-4d27-914a-91399e9639e5	Secondary	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AWS	FreeRTOS-Plus-TCP	affected 4.0.0 4.2.6 semver	Not specified
CNA	AWS	FreeRTOS-Plus-TCP	affected 4.3.0 4.4.1 semver	Not specified
CNA	AWS	FreeRTOS-Plus-TCP	unaffected 4.2.6	Not specified
CNA	AWS	FreeRTOS-Plus-TCP	unaffected 4.4.1	Not specified

References

Reference	Source	Link
aws.amazon.com/security/security-bulletins/2026-023-aws	ff89ba41-3aa1-4d27-914a-91399e9639e5	aws.amazon
github.com/FreeRTOS/FreeRTOS-Plus-TCP/releases/tag/V4.2.6	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
github.com/FreeRTOS/FreeRTOS-Plus-TCP/security/advisories/GHSA-gffr-xgjg...	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
github.com/FreeRTOS/FreeRTOS-Plus-TCP/releases/tag/V4.4.1	ff89ba41-3aa1-4d27-914a-91399e9639e5	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.