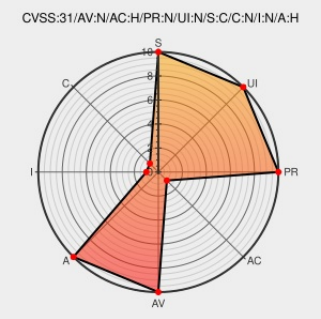
CVE-2020-10063

Published on: 06/05/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:34 PM UTC

CVE-2020-10063

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Zephyr from Zephyrproject contain the following vulnerability:

A remote adversary with the ability to send arbitrary CoAP packets to be parsed by Zephyr is able to cause a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.

CVE-2020-10063 has been assigned by vulnerabilities@zephyrproject.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **zephyrproject-rtos** - **zephyr** version **>= 2.2.0**

Affected Vendor/Software: **zephyrproject-rtos** - **zephyr** version **>= 2.1.0**

Affected Vendor/Software: **zephyrproject-rtos** - **zephyr** version **>= 1.14.0**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[Backport v1.14] net: coap: Fix possible overflow by ceolin · Pull Request #24530 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/24530
[ZEPSEC-55] Remote Denial of Service in CoAP Option Parsing Due To Integer Overflow - Zephyr Project Security Issues	Permissions Required zephyrprojectsec.atlassian.net text/html	MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-55
[Backport v2.1] net: coap: Fix possible overflow by ceolin · Pull Request #24535 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/24535
Vulnerabilities — Zephyr Project Documentation	Vendor Advisory docs.zephyrproject.org text/html	MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10063
Fix possible integer overflow in CoAP by ceolin · Pull Request #24435 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/24435
[Backport v2.2] net: coap: Fix possible overflow by ceolin · Pull Request #24531 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/24531

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Zephyrproject	Zephyr	All	All	All	All

cpe:2.3:o:zephyrproject:zephyr:*:*:*:*:*:*:*:*:

Discovery Credit

NCC Group for report

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report