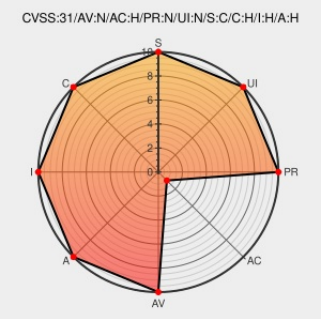
CVE-2020-10022

Published on: 05/11/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:33 PM UTC

CVE-2020-10022

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



Certain versions of Zephyr from Zephyrproject contain the following vulnerability:

A malformed JSON payload that is received from an UpdateHub server may trigger memory corruption in the Zephyr OS. This could result in a denial of service in the best case, or code execution in the worst case. See NCC-NCC-016 This issue affects: zephyrproject-rtos zephyr version 2.1.0 and later versions. version 2.2.0 and later versions.

CVE-2020-10022 has been assigned by vulnerabilities@zephyrproject.org to track the vulnerability - currently rated as CRITICAL severity.

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

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

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
lib: updatehub: Improve security by nandojve · Pull Request #24154 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/24154
Vulnerabilities — Zephyr Project Documentation	docs.zephyrproject.org text/html	MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10022
[ZEPSEC-28] UpdateHub Module Copies a Variable-Size Hash String Into a Fixed-Size Array - Zephyr Project Security Issues	Third Party Advisory zephyrprojectsec.atlassian.net text/html	MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-28
[backport v2.2] lib: updatehub: Minor bug fixes by otavio · Pull Request #24066 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/24066
[backport v2.1] lib: updatehub: Minor bug fixes by otavio · Pull Request #24065 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/24065

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	2.1.0	All	All	All
Operating System	Zephyrproject	Zephyr	2.2.0	All	All	All
Operating System	Zephyrproject	Zephyr	2.1.0	All	All	All
Operating System	Zephyrproject	Zephyr	2.2.0	All	All	All

cpe:2.3:o:zephyrproject:zephyr:2.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:zephyrproject:zephyr:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:o:zephyrproject:zephyr:2.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:zephyrproject:zephyr:2.2.0:*:*:*:*:*:*:*:

Discovery Credit

NCC Group for report

Social Mentions

Source	Title	Posted (UTC)
@kirurobo	弊学部で cluster を利用するとIPSにブロックされてしまう… なんとかならないものか。 TCP 1883 なので平文MQTTの中身かな？ JSONなら CVE-2020-10022 に判定されている可能性が高そう。	2022-12-14 04:02:46

← Previous ID

Next ID→