



CVE-2020-10022

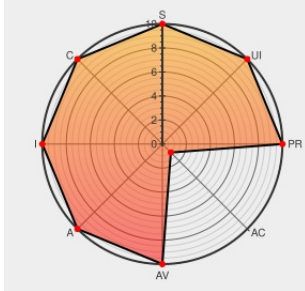
Published on: 05/11/2020 12:00:00 AM UTC

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

CVE-2020-10022

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H



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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)