



CVE-2020-10059

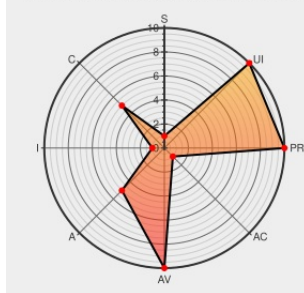
Published on: 05/11/2020 12:00:00 AM UTC

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

CVE-2020-10059

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

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



Certain versions of [Zephyr](#) from [Zephyrproject](#) contain the following vulnerability:

The UpdateHub module disables DTLS peer checking, which allows for a man in the middle attack. This is mitigated by firmware images requiring valid signatures. However, there is no benefit to using DTLS without the peer checking. See NCC-ZEP-018 This issue affects: zephyrproject-rtos zephyr version 2.1.0 and later versions.

CVE-2020-10059 has been assigned by [vulnerabilities@zephyrproject.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [zephyrproject-rtos](#) - [zephyr](#) version $\geq 2.1.0$

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

[backport 24954] updatehub: Require peer verification with DTLS by d3zd3z · Pull Request #24999 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/24999
[ZEPSEC-36] UpdateHub Module Explicitly Disables TLS Verification - Zephyr Project Security Issues	Third Party Advisory zephyrprojectsec.atlassian.net text/html	 MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-36
Vulnerabilities — Zephyr Project Documentation	docs.zephyrproject.org text/html	 MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10059
[backport 24954] updatehub: Require peer verification with DTLS by d3zd3z · Pull Request #24997 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/24997
updatehub: Require peer verification with DTLS by d3zd3z · Pull Request #24954 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/24954

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

© [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](#)