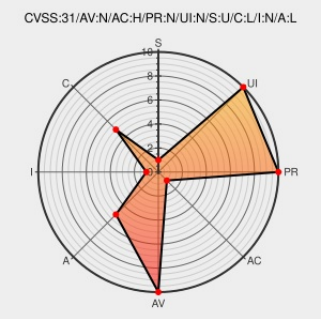
CVE-2020-10059

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



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 **>= 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

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

← Previous ID

Next ID→

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