

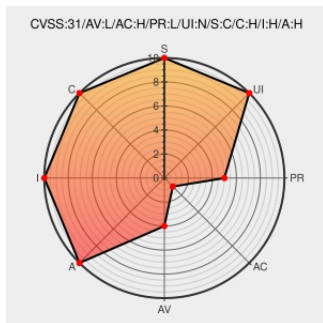


CVE-2020-10058

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

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

CVE-2020-10058

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

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

Multiple syscalls in the Kscan subsystem perform insufficient argument validation, allowing code executing in userspace to potentially gain elevated privileges. See NCC-ZEP-006 This issue affects: zephyrproject-rtos zephyr version 2.1.0 and later versions.

CVE-2020-10058 has been assigned by [vulnerabilities@zephyrproject.org](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [zephyrproject-rtos](#) - [zephyr](#) version **>= 2.1.0**

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
drivers: kscan: fix syscall handlers by ceolin · Pull Request #23748 · zephyrproject-	Patch Third Party Advisory	MISC github.com/zephyrproject-rtos/zephyr/pull/23748

Pull Request #23308 · Zephyrproject-rtos/zephyr · GitHub	Third Party Advisory github.com text/html	
fix some incorrect syscall handlers by andrewboie · Pull Request #23308 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/23308
[ZEPSEC-34] Multiple Syscalls In kscan Subsystem Performs No Argument Validation - Zephyr Project Security Issues	Third Party Advisory zephyrprojectsec.atlassian.net text/html	 MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-34
Vulnerabilities — Zephyr Project Documentation	docs.zephyrproject.org text/html	 MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10058

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

Discovery Credit

NCC Group for report

[← Previous ID](#)

[Next ID →](#)