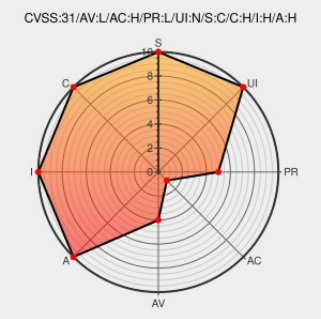
CVE-2020-10027

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

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

CVE-2020-10027

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



Certain versions of Zephyr from Zephyrproject contain the following vulnerability:

An attacker who has obtained code execution within a user thread is able to elevate privileges to that of the kernel. See NCC-ZEP-001 This issue affects: zephyrproject-rtos zephyr version 1.14.0 and later versions. version 2.1.0 and later versions.

CVE-2020-10027 has been assigned by vulnerabilities@zephyrproject.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **zephyrproject-rtos** - **zephyr** version **>= 1.14.0**

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: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

Vulnerabilities — Zephyr Project Documentation	docs.zephyrproject.org text/html	MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10027
arch: arc: fix the bug of blt in syscall by vonhust · Pull Request #23328 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/23328
backport-v2.1: arch: arc: fix the bug of blt in syscall by d3zd3z · Pull Request #23499 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/23499
backport-v1.14: arch: arc: fix the bug of blt in syscall by d3zd3z · Pull Request #23500 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/23500
[ZEPSEC-35] ARC Platform Uses Signed Integer Comparison When Validating Syscall Numbers - Zephyr Project Security Issues	Third Party Advisory zephyrprojectsec.atlassian.net text/html	MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-35

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	1.14.0	All	All	All
Operating System	Zephyrproject	Zephyr	2.1.0	All	All	All
Operating System	Zephyrproject	Zephyr	1.14.0	All	All	All
Operating System	Zephyrproject	Zephyr	2.1.0	All	All	All

cpe:2.3:o:zephyrproject:zephyr:1.14.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:zephyrproject:zephyr:1.14.0:*:*:*:*:*:*:*:

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

Discovery Credit

NCC Group for report

← Previous ID

Next ID→