CVE-2020-10067

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-10067
State	PUBLIC
Assigner	vulnerabilities@zephyrproject.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-11 23:15:00 UTC
Updated	2020-06-05 18:15:00 UTC
Description	A malicious userspace application can cause a integer overflow and bypass security checks performed by system call hand

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Zephyrproject	Zephyr	1.14.1	All	All	All
Operating System	Zephyrproject	Zephyr	2.1.0	All	All	All
Operating System	Zephyrproject	Zephyr	1.14.1	All	All	All
Operating System	Zephyrproject	Zephyr	2.1.0	All	All	All

References

Reference
[ZEPSEC-27] Integer Overflow In is_in_region Allows User Thread To Access Kernel Memory - Zephyr Project Security Issues
Vulnerabilities — Zephyr Project Documentation
Backport v1.14: syscalls: arm: Fix possible overflow in is_in_region function by ceolin · Pull Request #23653 · zephyrproject-rtos/zephyr · GitH
Backport v2.1: syscalls: arm: Fix possible overflow in is_in_region function by ceolin · Pull Request #23654 · zephyrproject-rtos/zephyr · GitHu
syscalls: arm: Fix possible overflow in is_in_region function by ceolin · Pull Request #23239 · zephyrproject-rtos/zephyr · GitHub
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: NCC Group for report

There are currently no legacy QID mappings associated with this CVE.

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