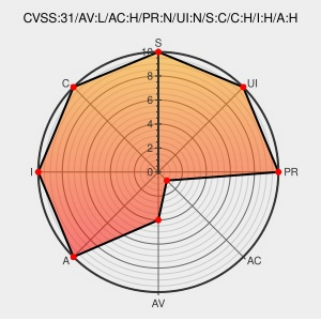
CVE-2020-10019

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

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

CVE-2020-10019

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



Certain versions of Zephyr from Zephyrproject contain the following vulnerability:

USB DFU has a potential buffer overflow where the requested length (wLength) is not checked against the buffer size. This could be used by a malicious USB host to exploit the buffer overflow. See NCC-ZEP-002 This issue affects: zephyrproject-rtos zephyr version 1.14.1 and later versions. version 2.1.0 and later versions.

CVE-2020-10019 has been assigned by vulnerabilities@zephyrproject.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **zephyrproject-rtos** - **zephyr** version **>= 1.14.1**

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
Vulnerabilities — Zephyr Project Documentation	docs.zephyrproject.org text/html	MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10019
usb: dfu: check requested length (wLength) during DFU_UPLOAD by jfischer-no · Pull Request #23190 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/23190
[v2.1-branch] usb: dfu: check requested length (wLength) during DFU_UPLOAD by d3zd3z · Pull Request #23457 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/23457
[ZEPSEC-25] Buffer Overflow in USB DFU requested length - Zephyr Project Security Issues	Third Party Advisory zephyrprojectsec.atlassian.net text/html	MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-25
Backport: usb: dfu: check requested length (wLength) during DFU_UPLOAD by d3zd3z · Pull Request #23460 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/pull/23460

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	All	All	All	All
Operating System	Zephyrproject	Zephyr	All	All	All	All
Operating System	Zephyrproject	Zephyr	All	All	All	All

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

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

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

Discovery Credit

NCC Group for report

← Previous ID

Next ID→

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