

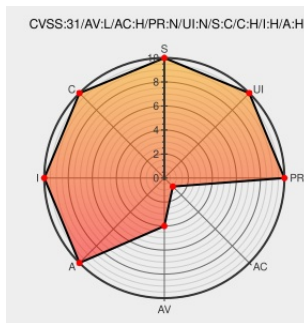


CVE-2020-10019

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

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	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](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)