

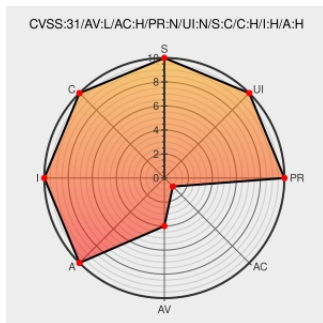


CVE-2020-10061

Published on: 06/05/2020 12:00:00 AM UTC

Last Modified on: 10/18/2021 12:35:00 PM UTC

CVE-2020-10061

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

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

Improper handling of the full-buffer case in the Zephyr Bluetooth implementation can result in memory corruption. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.

CVE-2020-10061 has been assigned by [vulnerabilities@zephyrproject.org](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [zephyrproject-rtos](#) - **zephyr** version **>= 2.2.0**

Affected Vendor/Software: [zephyrproject-rtos](#) - **zephyr** version **>= 1.14.0**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

[backport v1.14] Bluetooth: controller: legacy: Backport v2.2 to v1.14-branch by cvinayak · Pull Request #23091 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/23091
Vulnerabilities — Zephyr Project Documentation	Vendor Advisory docs.zephyrproject.org text/html	 MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10061
Bluetooth: controller: split: Fix regression handling invalid packet sequence by cvinayak · Pull Request #23516 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/23516
[backport v2.2] Bluetooth: controller: split: Fix regression in handling invalid pkt seq by cvinayak · Pull Request #23547 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/23547
[ZEPSEC-75] Error handling invalid packet sequence - Zephyr Project Security Issues	Third Party Advisory zephyrprojectsec.atlassian.net text/html	 MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-75
Bluetooth: controller: legacy: Fix regression handling tx pool corruption by cvinayak · Pull Request #23517 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/23517

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

Discovery Credit

PhD - Garbelini Matheus Eduardo

Social Mentions

Source	Title	Posted (UTC)
← Previous IDNext 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](#)