



CVE-2020-10068

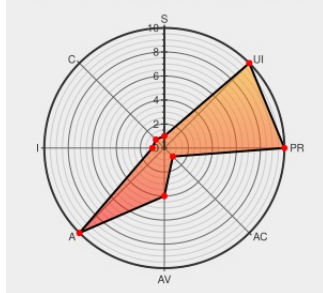
Published on: 06/05/2020 12:00:00 AM UTC

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

CVE-2020-10068

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

CVSS:31/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



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

In the Zephyr project Bluetooth subsystem, certain duplicate and back-to-back packets can cause incorrect behavior, resulting in a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.

CVE-2020-10068 has been assigned by [vulnerabilities@zephyrproject.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

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

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

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

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

CVE References

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

Vulnerabilities — Zephyr Project Documentation	Vendor Advisory docs.zephyrproject.org text/html	 MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10068
[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
Bluetooth: controller: legacy: Fix DLE duplicate requests by cvinayak · Pull Request #23708 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/23708
[backport v2.2] Bluetooth: controller: split: Fix DLE duplicate requests by cvinayak · Pull Request #23964 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/23964
[ZEPSEC-78] Zephyr Bluetooth DLE duplicate requests vulnerability - Zephyr Project Security Issues	Third Party Advisory zephyrprojectsec.atlassian.net text/html	 MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-78
Bluetooth: controller: split: Fix DLE duplicate requests by cvinayak · Pull Request #23707 · zephyrproject-rtos/zephyr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/zephyrproject-rtos/zephyr/pull/23707

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

[← Previous ID](#)

[Next ID →](#)

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](#)