



# stm32: usb: Infinite while loop in Interrupt Handler

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-4179
<b>State</b>	PUBLISHED
<b>Assigner</b>	zephyr
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-16 14:19:58 UTC
<b>Updated</b>	2026-04-02 20:45:41 UTC
<b>Description</b>	Issues in stm32 USB device driver (drivers/usb/device/usb_dc_stm32.c) can lead to an infinite while loop.

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from vulnerabilities@zephyrproject.org

**CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H**

**EPSS:** 0.000060000 probability, percentile 0.003350000 (date 2026-04-02)

**Problem Types:** CWE-835 | CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

Version	Source	Type	Score	Severity	Vector
3.1	vulnerabilities@zephyrproject.org	Secondary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H

#### NVD Known Affected Configurations (CPE 2.3)

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Zephyrproject-rtos	Zephyr	affected * 4.3 git	Not specified

#### References

Reference	Source	Link	T
github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-9xg7-g3q3-...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	E
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

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](https://status.cve.report)