



# CVE-2023-4264

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

## Summary

<b>CVE</b>	CVE-2023-4264
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnerabilities@zephyrproject.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-27 15:19:00 UTC
<b>Updated</b>	2023-11-14 03:15:00 UTC
<b>Description</b>	Potential buffer overflow vulnerabilities n the Zephyr Bluetooth subsystem.

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link
Full Disclosure: HNS-2023-03 - HN Security Advisory - Multiple vulnerabilities in Zephyr RTOS		<a href="#">seclists.org</a>
<a href="#">packetstormsecurity.com/files/175657/Zephyr-RTOS-3.x.0-Buffer-Overflows.html</a>		<a href="#">packetstormsecurity.com</a>
oss-security - HNS-2023-03 - HN Security Advisory - Multiple vulnerabilities in Zephyr RTOS		<a href="#">www.openwall.com</a>
Buffer overflow vulnerabilities in the Zephyr Bluetooth subsystem · Advisory · zephyrproject-rtos/zephyr · GitHub	MISC	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)