



CVE-2020-10070

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

Summary

CVE	CVE-2020-10070
State	PUBLIC
Assigner	vulnerabilities@zephyrproject.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-05 18:15:00 UTC
Updated	2020-06-12 14:27:00 UTC
Description	In the Zephyr Project MQTT code, improper bounds checking can result in memory corruption and possibly remote code ex

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
Vulnerabilities — Zephyr Project Documentation	MISC	docs.zephyrproject.org
net: mqtt: Several bugfixes by rlubos · Pull Request #23821 · zephyrproject-rtos/zephyr · GitHub	MISC	github.com
[ZEPSEC-85] MQTT buffer overflow on receive buffer - Zephyr Project Security Issues	MISC	zephyrprojectsec.atlassian.net
Research Report – Zephyr and MCUboot Security Assessment – NCC Group Research	MISC	research.nccgroup.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: NCC Group for report

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](#)