

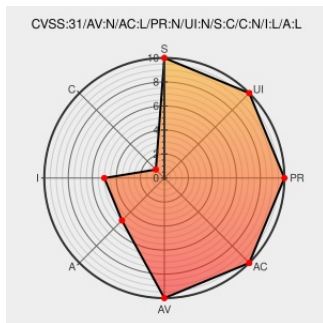


CVE-2022-1841

Published on: Not Yet Published

Last Modified on: 09/07/2022 04:54:00 PM UTC

CVE-2022-1841

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

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

In `subsys/net/ip/tcp.c` , function `tcp_flags` , when the incoming parameter flags is ECN or CWR , the buf will out-of-bounds write a byte zero.

CVE-2022-1841 has been assigned by [vulnerabilities@zephyrproject.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [zephyrproject-rtos](#) - [zephyr](#) version `<= v3.0`

CVSS3 Score: **5.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Out-of-Bound Write in <code>tcp_flags</code> · Advisory · zephyrproject-rtos/zephyr · GitHub	github.com text/html	MISC github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-5c3j-p8cr-2pgh

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
cpe:2.3:o:zephyrproject:zephyr:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
 @CVereport	CVE-2022-1841 : In subsys/net/ip/tcp.c , function tcp_flags , when the incoming parameter flags is ECN or CWR , the... twitter.com/i/web/status/1...					2022-08-31 19:46:50
 /r/netcve	CVE-2022-1841					2022-08-31 20:38:41
← Previous ID			Next ID →			