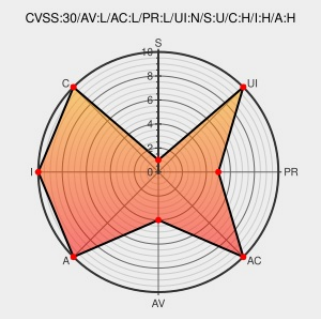
# CVE-2017-14202

Published on: 08/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:45 PM UTC

## CVE-2017-14202

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Zephyr from Zephyrproject contain the following vulnerability:

Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in the shell component of Zephyr allows a serial or telnet connected user to cause a crash, possibly with arbitrary code execution. This issue affects: Zephyr shell versions prior to 1.14.0 on all.

CVE-2017-14202 has been assigned by vulnerabilities@zephyrproject.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Zephyr** - **shell** version **prior to 1.14.0**

### CVSS3 Score: 7.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 4.6 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

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

| | | |
|---|---|---|
| [ZEPSEC-18] Buffer overflow in shell history - Zephyr Project Security Issues | Broken Link<br>zephyrprojectsec.atlassian.net<br>text/html | MISC<br>zephyrprojectsec.atlassian.net/browse/ZEPSEC-18 |
| Zephyr Kernel 1.14.0 — Zephyr Project Documentation | Release Notes<br>Vendor Advisory<br>docs.zephyrproject.org<br>text/html | MISC<br>docs.zephyrproject.org/1.14.0/releases/release-notes-1.14.html |
| shell: Allocate proper amount of history slab memory by agross-oss · Pull Request #13048 · zephyrproject-rtos/zephyr · GitHub | Patch<br>Third Party Advisory<br>github.com<br>text/html | MISC github.com/zephyrproject-rtos/zephyr/pull/13048 |

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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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**