



# CVE-2020-10060

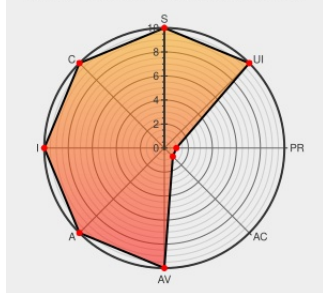
Published on: 05/11/2020 12:00:00 AM UTC

Last Modified on: 10/18/2021 12:35:00 PM UTC

## CVE-2020-10060

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

CVSS:31/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H



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

In `updatehub_probe`, right after JSON parsing is complete, `objects\[1]` is accessed from the output structure in two different places. If the JSON contained less than two elements, this access would reference uninitialized stack memory. This could result in a crash, denial of service, or possibly an information leak. Provided the fix in CVE-2020-10059 is applied, the attack requires compromise of the server. See NCC-ZEP-030 This issue affects: `zephyrproject-rtos zephyr` version 2.1.0 and later versions. version 2.2.0 and later versions.

CVE-2020-10060 has been assigned by [vulnerabilities@zephyrproject.org](mailto:vulnerabilities@zephyrproject.org) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [zephyrproject-rtos](#) - `zephyr` version `>= 2.1.0`

Affected Vendor/Software: [zephyrproject-rtos](#) - `zephyr` version `>= 2.2.0`

CVSS3 Score: **6.5 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>HIGH</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5.5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                                                                                     | Tags                                                                                                                | Link                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ZEPSEC-37] UpdateHub Might Dereference An Uninitialized Pointer - Zephyr Project Security Issues                                                               | <a href="#">Third Party Advisory</a><br><a href="#">zephyrprojectsec.atlassian.net</a><br><a href="#">text/html</a> |  <a href="#">MISC zephyrprojectsec.atlassian.net/browse/ZEPSEC-37</a>                            |
| mgmt: updatehub: Fix possible deref an uninitialized ptr by nandojve · Pull Request #27865 · zephyrproject-rtos/zephyr · GitHub                                 | <a href="#">github.com</a><br><a href="#">text/html</a>                                                             |  <a href="#">CONFIRM github.com/zephyrproject-rtos/zephyr/pull/27865</a>                         |
| Vulnerabilities — Zephyr Project Documentation                                                                                                                  | <a href="#">docs.zephyrproject.org</a><br><a href="#">text/html</a>                                                 |  <a href="#">MISC docs.zephyrproject.org/latest/security/vulnerabilities.html#cve-2020-10060</a> |
| [backport v2.2] lib: updatehub: Improve download on slow networks and apply security fix by nandojve · Pull Request #27891 · zephyrproject-rtos/zephyr · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a>                                                             |  <a href="#">CONFIRM github.com/zephyrproject-rtos/zephyr/pull/27891</a>                         |
| [backport v2.3] lib: updatehub: Fix possible deref an uninitialized ptr by nandojve · Pull Request #27889 · zephyrproject-rtos/zephyr · GitHub                  | <a href="#">github.com</a><br><a href="#">text/html</a>                                                             |  <a href="#">CONFIRM github.com/zephyrproject-rtos/zephyr/pull/27889</a>                         |
| [backport v2.1] lib: updatehub: Improve download on slow networks and apply security fix by nandojve · Pull Request #27893 · zephyrproject-rtos/zephyr · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a>                                                             |  <a href="#">CONFIRM github.com/zephyrproject-rtos/zephyr/pull/27893</a>                         |

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](mailto: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                            | <a href="#">Zephyrproject</a> | <a href="#">Zephyr</a> | All     | All    | All     | All      |
| Operating System                            | <a href="#">Zephyrproject</a> | <a href="#">Zephyr</a> | 2.1.0   | All    | All     | All      |
| Operating System                            | <a href="#">Zephyrproject</a> | <a href="#">Zephyr</a> | 2.2.0   | All    | All     | All      |
| Operating System                            | <a href="#">Zephyrproject</a> | <a href="#">Zephyr</a> | 2.1.0   | All    | All     | All      |
| Operating System                            | <a href="#">Zephyrproject</a> | <a href="#">Zephyr</a> | 2.2.0   | All    | All     | All      |
| cpe:2.3:o:zephyrproject:zephyr:*****:       |                               |                        |         |        |         |          |
| cpe:2.3:o:zephyrproject:zephyr:2.1.0:*****: |                               |                        |         |        |         |          |
| cpe:2.3:o:zephyrproject:zephyr:2.2.0:*****: |                               |                        |         |        |         |          |

| cpe:2.3:0:zephyrproject:zephyr:2.2.0: . . . . . |       |              |
|-------------------------------------------------|-------|--------------|
| cpe:2.3:0:zephyrproject:zephyr:2.1.0:*:*:*:*:*: |       |              |
| cpe:2.3:0:zephyrproject:zephyr:2.2.0:*:*:*:*:*: |       |              |
| Discovery Credit                                |       |              |
| NCC Group for report                            |       |              |
| Social Mentions                                 |       |              |
| Source                                          | Title | Posted (UTC) |
| <div>← Previous ID</div> <div>Next ID→</div>    |       |              |