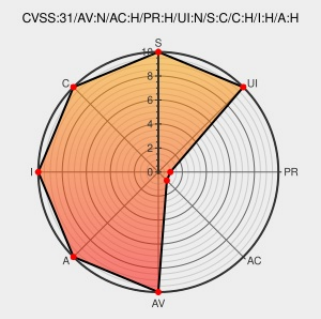
CVE-2020-10060

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



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 unitialized 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 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
NETWORK	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	HIGH

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

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

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	2.1.0	All	All	All
Operating System	Zephyrproject	Zephyr	2.2.0	All	All	All
Operating System	Zephyrproject	Zephyr	2.1.0	All	All	All
Operating System	Zephyrproject	Zephyr	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:o:zephyrproject:zephyr:2.1.0:*:*:*:*:*:*:*

cpe:2.3:o:zephyrproject:zephyr:2.2.0:*:*:*:*:*:*:*

Discovery Credit

NCC Group for report

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→