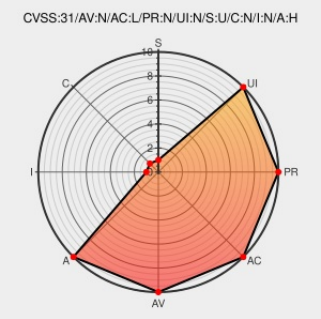
CVE-2020-12885

Published on: 06/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:35 PM UTC

CVE-2020-12885

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



Certain versions of Mbed Os from Arm contain the following vulnerability:

An infinite loop was discovered in the CoAP library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse_multiple_options() parses CoAP options in a while loop. This loop's exit condition is computed using the previously allocated heap memory required for storing the result of parsing multiple options. If the input heap memory calculation results in zero bytes, the loop exit condition is never met and the loop is not terminated. As a result, the packet parsing function never exits, leading to resource consumption.

CVE-2020-12885 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Bugfix/coap parser mem access bugs by mjurczak · Pull Request #116 · ARMmbed/mbed-coap · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/ARMmbed/mbed-coap/pull/116
Infinite loop in MbedOS CoAP library parser · Issue #12929 · ARMmbed/mbed-os · GitHub	Third Party Advisory github.com text/html	MISC github.com/ARMmbed/mbed-os/issues/12929

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Arm	Mbed Os	5.15.3	All	All	All
Operating System	Arm	Mbed Os	5.15.3	All	All	All

cpe:2.3:o:arm:mbed_os:5.15.3:*:*:*:*:*:*:*:

cpe:2.3:o:arm:mbed_os:5.15.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→