



CVE-2019-17212

Published on: 11/05/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:37 PM UTC

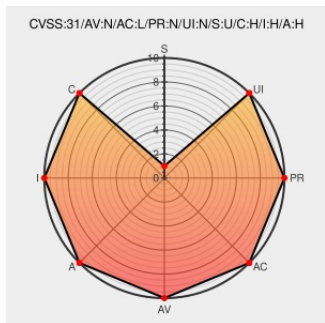
CVE-2019-17212

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Buffer overflows were discovered in the CoAP library in Arm Mbed OS 5.14.0. The CoAP parser is responsible for parsing received CoAP packets. The function `sn_coap_parser_options_parse()` parses CoAP input linearly using a while loop. Once an option is parsed in a loop, the current point (`*packet_data_pptr`) is increased correspondingly. The pointer is restricted by the size of the received buffer, as well as by the

0xFF delimiter byte. Inside each while loop, the check of the value of `*packet_data_pptr` is not strictly enforced. More specifically, inside a loop, `*packet_data_pptr` could be increased and then dereferenced without checking. Moreover, there are many other functions in the format of `sn_coap_parser_****()` that do not check whether the pointer is within the bounds of the allocated buffer. All of these lead to heap-based or stack-based buffer overflows, depending on how the CoAP packet buffer is allocated.

CVE-2019-17212 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

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

CVE References

Description	Tags	Link
mbed-os/sn_coap_parser.c at d91ed5fa42ea0f32e4422a3c562e7b045a17da40 · ARMmbed/mbed-os · GitHub	Third Party Advisory github.com text/html	MISC github.com/ARMmbed/mbed-os/blob/d91ed5fa42ea0f32e4422a3c562e7b045a17da40/features/fr-coap/source/sn_coap_parser.c#L301
mbed-os/sn_coap_parser.c at d91ed5fa42ea0f32e4422a3c562e7b045a17da40 · ARMmbed/mbed-os · GitHub	Third Party Advisory github.com text/html	MISC github.com/ARMmbed/mbed-os/blob/d91ed5fa42ea0f32e4422a3c562e7b045a17da40/features/fr-coap/source/sn_coap_parser.c#L331
mbed-os/sn_coap_parser.c at d91ed5fa42ea0f32e4422a3c562e7b045a17da40 · ARMmbed/mbed-os · GitHub	Third Party Advisory github.com text/html	MISC github.com/ARMmbed/mbed-os/blob/d91ed5fa42ea0f32e4422a3c562e7b045a17da40/features/fr-coap/source/sn_coap_parser.c#L257
mbed-os/sn_coap_parser.c at d91ed5fa42ea0f32e4422a3c562e7b045a17da40 · ARMmbed/mbed-os · GitHub	Third Party Advisory github.com text/html	MISC github.com/ARMmbed/mbed-os/blob/d91ed5fa42ea0f32e4422a3c562e7b045a17da40/features/fr-coap/source/sn_coap_parser.c#L310
mbed-os/sn_coap_parser.c at d91ed5fa42ea0f32e4422a3c562e7b045a17da40 · ARMmbed/mbed-os · GitHub	Third Party Advisory github.com text/html	MISC github.com/ARMmbed/mbed-os/blob/d91ed5fa42ea0f32e4422a3c562e7b045a17da40/features/fr-coap/source/sn_coap_parser.c#L660
memory access out of range in MbedOS CoAP library parser part · Issue #11803 · ARMmbed/mbed-os · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/ARMmbed/mbed-os/issues/11803
mbed-os/sn_coap_parser.c at d91ed5fa42ea0f32e4422a3c562e7b045a17da40 · ARMmbed/mbed-os · GitHub	Third Party Advisory github.com text/html	MISC github.com/ARMmbed/mbed-os/blob/d91ed5fa42ea0f32e4422a3c562e7b045a17da40/features/fr-coap/source/sn_coap_parser.c#L313

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	Mbed	Mbed	5.13.2	All	All	All
Operating System	Mbed	Mbed	5.14.0	All	All	All
Operating System	Mbed	Mbed	5.13.2	All	All	All
Operating System	Mbed	Mbed	5.14.0	All	All	All
cpe:2.3:o:mbed:mbed:5.13.2:*:*:*:*:*						
cpe:2.3:o:mbed:mbed:5.14.0:*:*:*:*:*						

cpe:2.3:o:MBED:MBED:5.13.2:*:*:*:*:*:

cpe:2.3:o:MBED:MBED:5.14.0:*:*:*:*:*:

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 registered 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](#)