

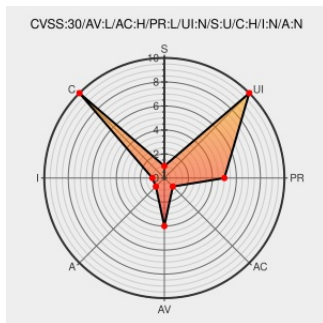


CVE-2018-19608

Published on: 12/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:39 PM UTC

CVE-2018-19608

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

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

Arm Mbed TLS before 2.14.1, before 2.7.8, and before 2.1.17 allows a local unprivileged attacker to recover the plaintext of RSA decryption, which is used in RSA-without-(EC)DH(E) cipher suites.

CVE-2018-19608 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.7 - MEDIUM**

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

CVSS2 Score: **1.9 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Mbed TLS Security Advisory 2018-03 - Tech Updates - mbed TLS (Previously PolarSSL)	Third Party Advisory tls.mbed.org text/html	CONFIRM tls.mbed.org/tech-updates/security-advisories/mbedtls-security-advisory-2018-03
Your browser does not support frames. We recommend	Third Party Advisory	MISC cat.eyalro.net/

upgrading your browser.

cat.eyalro.net

text/html

Mbed TLS 2.14.1, 2.7.8 and 2.1.17 released - Tech Updates
- Mbed TLS (Previously PolarSSL)

Third Party Advisory

tls.mbed.org

text/html

 [CONFIRM tls.mbed.org/tech-updates/releases/mbedtls-2.14.1-2.7.8-and-2.1.17-released](https://tls.mbed.org/tech-updates/releases/mbedtls-2.14.1-2.7.8-and-2.1.17-released)

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.

Related QID Numbers

[500393](#) Alpine Linux Security Update for mbedtls

[690317](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mbed Transport Layer Security (TLS) (293f40a0-ffa1-11e8-b258-0011d823eebd)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Mbed Tls	All	All	All	All
Application	Arm	Mbed Tls	All	All	All	All

cpe:2.3:a:arm:mbed_tls:*****:

cpe:2.3:a:arm:mbed_tls:*****:

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](#)