



# CVE-2018-0488

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                      |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2018-0488                                                                                                        |
| <b>State</b>           | PUBLIC                                                                                                               |
| <b>Assigner</b>        | security@debian.org                                                                                                  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                         |
| <b>Published</b>       | 2018-02-13 15:29:00 UTC                                                                                              |
| <b>Updated</b>         | 2020-08-24 17:37:00 UTC                                                                                              |
| <b>Description</b>     | ARM mbed TLS before 1.3.22, before 2.1.10, and before 2.7.0, when the truncated HMAC extension and CBC are used, all |

## Risk And Classification

### Problem Types: CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                      | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Application      | <a href="#">Arm</a>    | <a href="#">Mbed Tls</a>     | All     | All    | All     | All      |
| Application      | <a href="#">Arm</a>    | <a href="#">Mbed Tls</a>     | All     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |

## References

| Reference                                                            | Source  | Link                                                              | Tags                        |
|----------------------------------------------------------------------|---------|-------------------------------------------------------------------|-----------------------------|
| mbed TLS: Multiple vulnerabilites (GLSA 201804-19) — Gentoo Security | GENTOO  | <a href="https://security.gentoo.org">security.gentoo.org</a>     | Third Party Advisory        |
| Debian -- Security Information -- DSA-4147-1 polarssl                | DEBIAN  | <a href="https://www.debian.org">www.debian.org</a>               | Third Party Advisory        |
| Debian -- Security Information -- DSA-4138-1 mbedtls                 | DEBIAN  | <a href="https://www.debian.org">www.debian.org</a>               | Third Party Advisory        |
| USN-4267-1: ARM mbed TLS vulnerabilities   Ubuntu security notices   | UBUNTU  | <a href="https://usn.ubuntu.com">usn.ubuntu.com</a>               |                             |
| mbed TLS Security Advisory 2018-01 - Tech Updates                    | CONFIRM | <a href="https://tls.mbed.org">tls.mbed.org</a>                   | Mitigation, Vendor Advisory |
| ARM mbed TLS CVE-2018-0488 Remote Code Execution Vulnerability       | BID     | <a href="https://www.securityfocus.com">www.securityfocus.com</a> | Third Party Advisory, VDB   |
| CVE Program record                                                   | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                     | canonical                   |
| NVD vulnerability detail                                             | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, analysis         |

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[500401](#) Alpine Linux Security Update for mbedtls

[504160](#) Alpine Linux Security Update for mbedtls

[690637](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mbed Transport Layer Security (TLS) (polarssl) (c2f107e1-2493-11e8-b3e8-001cc0382b2f)

[710216](#) Gentoo Linux mbed Transport Layer Security Multiple vulnerabilities Vulnerability (GLSA 201804-19)

© [CVE.report](#) 2026 |

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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)