



CVE-2018-0497

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

Summary

CVE	CVE-2018-0497
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-28 17:29:00 UTC
Updated	2020-02-10 16:15:00 UTC
Description	ARM mbed TLS before 2.12.0, before 2.7.5, and before 2.1.14 allows remote attackers to achieve partial plaintext recovery

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arm	Mbed Tls	All	All	All	All
Application	Arm	Mbed Tls	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference	Source	Link	Tags
Mbed TLS Security Advisory 2018-02 - Tech Updates - Mbed TLS (Previously PolarSSL)	CONFIRM	tls.mbed.org	Mitigation, Third Party
USN-4267-1: ARM mbed TLS vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
Debian -- Security Information -- DSA-4296-1 mbedtls	DEBIAN	www.debian.org	Third Party Advice
[SECURITY] [DLA 1518-1] polarssl security update	MLIST	lists.debian.org	Mailing List, Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500392](#) Alpine Linux Security Update for mbedtls

[504150](#) Alpine Linux Security Update for mbedtls

[690622](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mbed Transport Layer Security (TLS) (f4876dd4-9ca8-11e8-aa17-0011d823eebd)

© [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](#)