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 P
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 Advisc
[SECURITY] [DLA 1518-1] polarssl security update	MLIST	lists.debian.org	Mailing List, Third
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

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)