CVE-2018-0487

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-0487
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-13 15:29:00 UTC
Updated	2020-02-10 16:15:00 UTC
Description	ARM mbed TLS before 1.3.22, before 2.1.10, and before 2.7.0 allows remote attackers to execute arbitrary code or cause a

Risk And Classification

Problem Types: CWE-119

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: Multiple vulnerabilites (GLSA 201804-19) — Gentoo Security	GENTOO	security.gentoo.org	Third Party Advisory
Debian -- Security Information -- DSA-4147-1 polarssl	DEBIAN	www.debian.org	Third Party Advisory
Debian -- Security Information -- DSA-4138-1 mbedtls	DEBIAN	www.debian.org	Third Party Advisory
USN-4267-1: ARM mbed TLS vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
ARM mbed TLS CVE-2018-0487 Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB
mbed TLS Security Advisory 2018-01 - Tech Updates	CONFIRM	tls.mbed.org	Mitigation, Vendor Advisory
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

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 vulnerabilites Vulnerability (GLSA 201804-19)