



CVE-2017-18187

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

Summary

CVE	CVE-2017-18187
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-14 17:29:00 UTC
Updated	2020-02-10 16:15:00 UTC
Description	In ARM mbed TLS before 2.7.0, there is a bounds-check bypass through an integer overflow in PSK identity parsing in the s

Risk And Classification

Problem Types: CWE-190

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
mbed TLS: Multiple vulnerabilites (GLSA 201804-19) — Gentoo Security	GENTOO	security.gentoo.org
Prevent bounds check bypass through overflow in PSK identity parsing · ARMmbed/mbedtls@83c9f49 · GitHub	CONFIRM	github.com
Debian -- Security Information -- DSA-4147-1 polarssl	DEBIAN	www.debian.org
mbedtls/ChangeLog at master · ARMmbed/mbedtls · GitHub	CONFIRM	github.com
Debian -- Security Information -- DSA-4138-1 mbedtls	DEBIAN	www.debian.org
USN-4267-1: ARM mbed TLS vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
ARM mbed TLS CVE-2017-18187 Integer Overflow Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org

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

[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