CVE-2026-34873

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-34873
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 21:17:01 UTC
Updated	2026-04-01 21:17:01 UTC
Description	An issue was discovered in Mbed TLS 3.5.0 through 4.0.0. Client impersonation can occur while resuming a TLS 1.3 sessic

Risk And Classification

Problem Types: n/a

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
mbed-tls.readthedocs.io/en/latest/security-advisories	cve@mitre.org	mbed-tls.readthedocs.io	
mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2026-...	cve@mitre.org	mbed-tls.readthedocs.io	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report