CVE-2026-25834

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-25834
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 18:16:28 UTC
Updated	2026-04-01 20:16:23 UTC
Description	Mbed TLS v3.3.0 up to 3.6.5 and 4.0.0 allows Algorithm Downgrade.

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

EPSS: 0.000260000 probability, percentile 0.072010000 (date 2026-04-02)

Problem Types: CWE-295 | CWE-327 | n/a | CWE-295 CWE-295 Improper Certificate Validation | CWE-327 CWE-327 Use of a Broken or Risky Cryptographic Algorithm

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

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.