VDB-354827 · CVE-2026-5246 · GCVE-100-354827

CESANTA MONGOOSE UP TO 7.20 P-384 PUBLIC KEY MONGOOSE.C MG_TLS_VERIFY_CERT_SIGNATURE AUTHORIZATION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.1	$0-$5k	1.22+

Summary

A vulnerability marked as critical has been reported in Cesanta Mongoose up to 7.20. Affected by this vulnerability is the function `mg_tls_verify_cert_signature` of the file *mongoose.c* of the component *P-384 Public Key Handler*. The manipulation leads to authorization. This vulnerability is uniquely identified as CVE-2026-5246. The attack is possible to be carried out remotely. Moreover, an exploit is present. It is suggested to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Details

A vulnerability, which was classified as critical, has been found in Cesanta Mongoose up to 7.20. This issue affects the function `mg_tls_verify_cert_signature` of the file *mongoose.c* of the component *P-384 Public Key Handler*. The manipulation with an unknown input leads to a authorization vulnerability. Using CWE to declare the problem leads to CWE-639. The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data. Impacted is confidentiality, integrity, and availability.

The identification of this vulnerability is CVE-2026-5246. The exploitation is known to be difficult. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details as well as a public exploit are known.

It is declared as proof-of-concept. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Upgrading to version 7.21 eliminates this vulnerability. The upgrade is hosted for download at github.com. Applying the patch 0d882f1b43ff2308b7486a56a9d60cd6dba8a3f1 is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

The entries VDB-354825 and VDB-354826 are pretty similar.

Product

Vendor

- Cesanta

Name

- Mongoose

Version

- 7.0
- 7.1
- 7.2
- 7.3
- 7.4
- 7.5
- 7.6
- 7.7
- 7.8
- 7.9
- 7.10
- 7.11
- 7.12
- 7.13
- 7.14

License

- open-source

Website

- Product: https://github.com/cesanta/mongoose/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.6
VulDB Meta Temp Score: 5.1

VulDB Base Score: 5.6
VulDB Temp Score: 5.1
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Authorization
CWE: CWE-639 / CWE-285 / CWE-266
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public

Status: Proof-of-Concept
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: Mongoose 7.21
Patch: 0d882f1b43ff2308b7486a56a9d60cd6dba8a3f1

Timeline

04/02/2026		Advisory disclosed
04/02/2026	+0 days	VulDB entry created
04/02/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Status: Confirmed

CVE: CVE-2026-5246 (🔒)
GCVE (CVE): GCVE-0-2026-5246
GCVE (VulDB): GCVE-100-354827
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/02/2026 09:48 AM
Changes: 04/02/2026 09:48 AM (60)
Complete: 🔍
Submitter: the_evilsocket
Cache ID: 172:DDD:179

Submit

Accepted

- Submit #770104: Cesanta Mongoose 7.20 Authorization Bypass (by the_evilsocket)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa