VDB-354826 · CVE-2026-5245 · GCVE-100-354826

CESANTA MONGOOSE UP TO 7.20 MDNS RECORD MONGOOSE.C HANDLE_MDNS_RECORD BUF STACK-BASED OVERFLOW

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

Summary

A vulnerability labeled as critical has been found in Cesanta Mongoose up to 7.20. Affected is the function `handle_mdns_record` of the file *mongoose.c* of the component *mDNS Record Handler*. Executing a manipulation of the argument *buf* can lead to stack-based overflow. This vulnerability is handled as CVE-2026-5245. The attack can be executed remotely. Additionally, an exploit exists. The affected component should be upgraded. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Details

A vulnerability classified as critical was found in Cesanta Mongoose up to 7.20. This vulnerability affects the function `handle_mdns_record` of the file *mongoose.c* of the component *mDNS Record Handler*. The manipulation of the argument `buf` with an unknown input leads to a stack-based overflow vulnerability. The CWE definition for the vulnerability is CWE-121. A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). As an impact it is known to affect confidentiality, integrity, and availability.

This vulnerability was named CVE-2026-5245. The exploitation appears to be difficult. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details and also 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.

Entries connected to this vulnerability are available at VDB-354825 and VDB-354827.

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: Stack-based overflow
CWE: CWE-121 / CWE-119
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-2026-5245 (🔒)
GCVE (CVE): GCVE-0-2026-5245
GCVE (VulDB): GCVE-100-354826
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 (61)
Complete: 🔍
Submitter: the_evilsocket
Cache ID: 172:34B:179

Submit

Accepted

- Submit #770103: Cesanta Mongoose 7.20 Stack-based Buffer Overflow (by the_evilsocket)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa