



# Cesanta Mongoose TLS 1.3 mongoose.c mg\_tls\_rcv\_cert heap-based overflow

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

## Summary

<b>CVE</b>	CVE-2026-5244
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulDB
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-02 08:16:28 UTC
<b>Updated</b>	2026-04-03 16:10:52 UTC
<b>Description</b>	A vulnerability has been found in Cesanta Mongoose up to 7.20. This affects the function mg_tls_rcv_cert of the file mong

## Risk And Classification

**Primary CVSS:** v4.0 6.9 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000580000 probability, percentile 0.182250000 (date 2026-04-02)

**Problem Types:** CWE-119 | CWE-122 | CWE-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

### CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cesanta	Mongoose	affected 7.0	Not specified
CNA	Cesanta	Mongoose	affected 7.1	Not specified
CNA	Cesanta	Mongoose	affected 7.2	Not specified
CNA	Cesanta	Mongoose	affected 7.3	Not specified
CNA	Cesanta	Mongoose	affected 7.4	Not specified
CNA	Cesanta	Mongoose	affected 7.5	Not specified
CNA	Cesanta	Mongoose	affected 7.6	Not specified
CNA	Cesanta	Mongoose	affected 7.7	Not specified
CNA	Cesanta	Mongoose	affected 7.8	Not specified
CNA	Cesanta	Mongoose	affected 7.9	Not specified
CNA	Cesanta	Mongoose	affected 7.10	Not specified
CNA	Cesanta	Mongoose	affected 7.11	Not specified
CNA	Cesanta	Mongoose	affected 7.12	Not specified
CNA	Cesanta	Mongoose	affected 7.13	Not specified
CNA	Cesanta	Mongoose	affected 7.14	Not specified
CNA	Cesanta	Mongoose	affected 7.15	Not specified
CNA	Cesanta	Mongoose	affected 7.16	Not specified
CNA	Cesanta	Mongoose	affected 7.17	Not specified
CNA	Cesanta	Mongoose	affected 7.18	Not specified

CNA	Cesanta	Mongoose	affected 7.19	Not specified
CNA	Cesanta	Mongoose	affected 7.20	Not specified
CNA	Cesanta	Mongoose	unaffected 7.21	Not specified

## References

Reference	Source	Link	Tags
vuldb.com/submit/770063	cna@vuldb.com	<a href="https://vuldb.com">vuldb.com</a>	
vuldb.com/vuln/354825/cti	cna@vuldb.com	<a href="https://vuldb.com">vuldb.com</a>	
vuldb.com/vuln/354825	cna@vuldb.com	<a href="https://vuldb.com">vuldb.com</a>	
github.com/cesanta/mongoose/releases/tag/7.21	cna@vuldb.com	<a href="https://github.com">github.com</a>	
github.com/cesanta/mongoose	cna@vuldb.com	<a href="https://github.com">github.com</a>	
github.com/cesanta/mongoose/commit/0d882f1b43ff2308b7486a56a9d60cd6dba8a3f1	cna@vuldb.com	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**CNA:** the\_evilsocket (VulDB User) (en)

**CNA:** VulDB (en)

## Additional Advisory Data

Source	Time	Event
CNA	2026-04-02T00:00:00.000Z	Advisory disclosed
CNA	2026-04-02T02:00:00.000Z	VulDB entry created
CNA	2026-04-02T09:48:19.000Z	VulDB entry last update

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

© 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)