



# Cesanta Mongoose GCM Authentication Tag tls\_aes128.c mg\_aes\_gcm\_decrypt signature verification

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

## Summary

<b>CVE</b>	CVE-2026-6986
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulDB
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-25 17:16:33 UTC
<b>Updated</b>	2026-04-25 17:16:33 UTC
<b>Description</b>	A security vulnerability has been detected in Cesanta Mongoose up to 7.20. This issue affects the function mg_aes_gcm_d

## Risk And Classification

**Primary CVSS:** v4.0 6.3 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/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

**Problem Types:** CWE-345 | CWE-347 | CWE-347 Improper Verification of Cryptographic Signature | CWE-345 Insufficient Verification of Data Authenticity

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/C
4.0	CNA	DECLARED	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
3.0	CNA	DECLARED	3.7	LOW	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	2.6		AV:N/AC:H/Au:N/C:N/I:P/A:N
2.0	CNA	DECLARED	2.6		AV:N/AC:H/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/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

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

### CVSS v3.0 Breakdown

Attack Vector

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/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	<a href="#">Cesanta</a>	<a href="#">Mongoose</a>	affected 7.19	Not specified
CNA	<a href="#">Cesanta</a>	<a href="#">Mongoose</a>	affected 7.20	Not specified
CNA	<a href="#">Cesanta</a>	<a href="#">Mongoose</a>	unaffected 7.21	Not specified

## References

Reference	Source	Link	Tags
<a href="https://vuldb.com/vuln/359529">vuldb.com/vuln/359529</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	
<a href="https://github.com/cesanta/mongoose/releases/tag/7.21">github.com/cesanta/mongoose/releases/tag/7.21</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://github.com">github.com</a>	
<a href="https://vuldb.com/submit/796231">vuldb.com/submit/796231</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	
<a href="https://vuldb.com/vuln/359529/cti">vuldb.com/vuln/359529/cti</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	
<a href="https://github.com/dwBruijn/CVEs/blob/main/Mongoose/AESGCM.md">github.com/dwBruijn/CVEs/blob/main/Mongoose/AESGCM.md</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<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:** [dwbruijn \(VulDB User\) \(en\)](#)

**CNA:** [VulDB CNA Team \(en\)](#)

## Additional Advisory Data

Source	Time	Event
CNA	2026-04-24T00:00:00.000Z	Advisory disclosed
CNA	2026-04-24T02:00:00.000Z	VulDB entry created
CNA	2026-04-24T21:18:01.000Z	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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

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