



CVE-2017-2921

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2017-2921
State	PUBLISHED
Assigner	talos
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-07 16:29:01 UTC
Updated	2025-04-20 01:37:25 UTC
Description	An exploitable memory corruption vulnerability exists in the Websocket protocol implementation of Cesanta Mongoose 6.8.

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

Problem Types: CWE-190 | denial of service

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	talos-cna@cisco.com	Secondary	8.1	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	CNA	DECLARED	8.1	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

ntegrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cesanta	Mongoose	6.8	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Cesanta	Mongoose	affected 6.8	Not specified		
References						
Reference				Source	Link	
TALOS-2017-0428 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence				af854a3a-2127-422b-91ae-364da2661108	www	
CVE Program record				CVE.ORG	www	
NVD vulnerability detail				NVD	nvd.	
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						