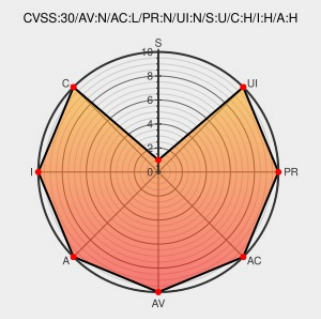
CVE-2017-2922

Published on: 11/07/2017 12:00:00 AM UTC

Last Modified on: 06/13/2022 07:16:00 PM UTC

CVE-2017-2922

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mongoose from Cesanta contain the following vulnerability:

An exploitable memory corruption vulnerability exists in the Websocket protocol implementation of Cesanta Mongoose 6.8. A specially crafted websocket packet can cause a buffer to be allocated while leaving stale pointers which leads to a use-after-free vulnerability which can be exploited to achieve remote code execution. An attacker needs to send a specially crafted websocket packet over the network to trigger this vulnerability.

CVE-2017-2922 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Cesanta** - **Mongoose** version **6.8**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

TALOS-2017-0429 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Technical Description Third Party Advisory www.talosintelligence.com text/html	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2017-0429

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cesanta	Mongoose	6.8	All	All	All
Application	Cesanta	Mongoose	6.8	All	All	All

cpe:2.3:a:cesanta:mongoose:6.8:*:*:*:*:*:*:*:

cpe:2.3:a:cesanta:mongoose:6.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→