



CVE-2017-2894

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

Last Modified on: 06/07/2022 05:24:00 PM UTC

CVE-2017-2894

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Mongoose](#) from [Cesanta](#) contain the following vulnerability:

An exploitable stack buffer overflow vulnerability exists in the MQTT packet parsing functionality of Cesanta Mongoose 6.8. A specially crafted MQTT SUBSCRIBE packet can cause a stack buffer overflow resulting in remote code execution. An attacker needs to send a specially crafted MQTT packet over the network to trigger this

vulnerability.

CVE-2017-2894 has been assigned by [cisco](#) talos-cna@cisco.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [cisco](#) **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
-------------	------	------

There are currently no QIDs associated with this CVE

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:****:****:						

Next ID→