



CVE-2018-18764

Published on: 10/28/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:52 PM UTC

CVE-2018-18764

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H



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

An exploitable arbitrary memory read vulnerability exists in the MQTT packet-parsing functionality of Cesanta Mongoose 6.13. It is a heap-based buffer over-read in a `parse_mqtt_getu16` call. A specially crafted MQTT SUBSCRIBE packet can cause an arbitrary out-of-bounds memory read potentially resulting in information disclosure and denial

of service. An attacker needs to send a specially crafted MQTT packet over the network to trigger this vulnerability.

CVE-2018-18764 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
DeChyMysel/Cesanta	CVE-2018-18764	MISC

PoCbyMyself/Cesanta
Mongoose MQTT getu16
heap buffer
overflow2.md at master ·
TiffanyBlue/PoCbyMyself
· GitHub

Exploit

Third Party Advisory

github.com

text/html

MISC

github.com/TiffanyBlue/PoCbyMyself/blob/master/mongoose6.13/mqtt/Cesanta%20Mongoo

PoCbyMyself/Cesanta
Mongoose MQTT getu16
heap buffer
overflow1.md at master ·
TiffanyBlue/PoCbyMyself
· GitHub

Exploit

Third Party Advisory

github.com

text/html

MISC

github.com/TiffanyBlue/PoCbyMyself/blob/master/mongoose6.13/mqtt/Cesanta%20Mongoo

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	6.13	All	All	All
Application	Cesanta	Mongoose	6.13	All	All	All
cpe:2.3:a:cesanta:mongoose:6.13:*:*:*:*:*:						
cpe:2.3:a:cesanta:mongoose:6.13:*:*:*:*:*:						

No vendor comments have been submitted for this CVE