



CVE-2018-20356

Published on: 06/10/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-20356

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

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

An invalid read of 8 bytes due to a use-after-free vulnerability in the `mg_http_free_proto_data_cgi` function call in `mongoose.c` in Cesanta Mongoose Embedded Web Server Library 6.13 and earlier allows a denial of service (application crash) or remote code execution.

CVE-2018-20356 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

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
mongoose-6.13-fuzz/Simplest_Web_Server_Use_After_Free-read_mg_http_free_proto_data_cgi.png at master · insi2304/mongoose-6.13-fuzz · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/insi2304/mongoose-6.13-fuzz/blob/master/Simplest_Web_Server_Use_After_Free-read_mg_http_free_proto_data_cgi.png

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	All	All	All	All
cpe:2.3:a:cesanta:mongoose:*****::						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→