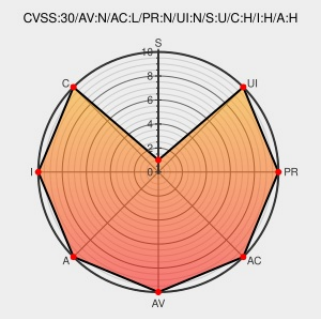
CVE-2017-2891

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

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

CVE-2017-2891

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



Certain versions of Mongoose from Cesanta contain the following vulnerability:

An exploitable use-after-free vulnerability exists in the HTTP server implementation of Cesanta Mongoose 6.8. An ordinary HTTP POST request with a CGI target can cause a reuse of previously freed pointer potentially resulting in remote code execution. An attacker needs to send this HTTP request over the network to trigger this vulnerability.

CVE-2017-2891 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-2017-0398 || Cisco Talos Intelligence Group -	Exploit	MISC

Comprehensive Threat Intelligence	Technical Description Third Party Advisory www.talosintelligence.com text/html	www.talosintelligence.com/vulnerability_reports/TALOS-2017-0398

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→