



# CVE-2021-26528

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-26528
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-08 21:15:00 UTC
<b>Updated</b>	2021-02-12 20:57:00 UTC
<b>Description</b>	The mg_http_serve_file function in Cesanta Mongoose HTTP server 7.0 is vulnerable to remote OOB write attack via connect

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cesanta</a>	<a href="#">Mongoose</a>	7.0	All	All	All
Application	<a href="#">Cesanta</a>	<a href="#">Mongoose</a>	7.0	All	All	All

## References

### Reference

- Out-of-bounds write caused by incorrect error handling of calloc in mg\_http\_serve\_file (mongoose.c:800) · Issue #1201 · cesanta/mongoose
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**