



# CVE-2021-33824

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

## Summary

<b>CVE</b>	CVE-2021-33824
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-18 20:15:00 UTC
<b>Updated</b>	2021-06-24 19:01:00 UTC
<b>Description</b>	An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attackers can use slowhttptest tool to send

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Moxa</a>	<a href="#">Mgate Mb3180</a>	-	All	All	All
Operating System	<a href="#">Moxa</a>	<a href="#">Mgate Mb3180 Firmware</a>	2.1	build_18113012	All	All

## References

Reference	Source	Link	Tags
<a href="#">CVE-POC/CVE-2021-33824.md at master · Jian-Xian/CVE-POC · GitHub</a>	MISC	<a href="#">github.com</a>	
<a href="#">GitHub - shekyan/slowhttptest: Application Layer DoS attack simulator</a>	MISC	<a href="#">github.com</a>	
<a href="#">MGate MB3180/MB3280/MB3480 Series - Modbus TCP Gateways   MOXA</a>	MISC	<a href="#">www.moxa.com</a>	
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">www.cve.org</a>	canonical
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)**