# CVE-2021-33824

## [Discoverer]

*Jian Xian Li, *Hao Hsiang Lin, Guan Yu Lai

Telecom Technology Center

(TTC is an experienced cybersecurity professional team. It helps companies to improve their security posture, and increase the confidence in implementing, and assessing the right security controls and vulnerabilities of network-connectable consumer/medical/industrial products.)

## [Description]

An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service.

## [Attack Type]

Remote

## [Product]

MOXA Mgate MB3180

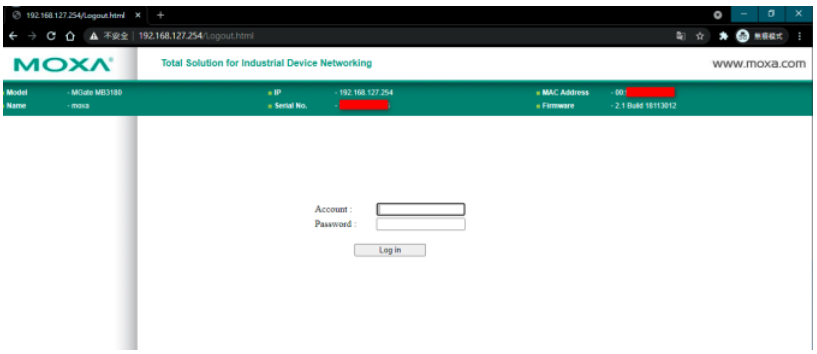
## [Version]

2.1 Build 18113012

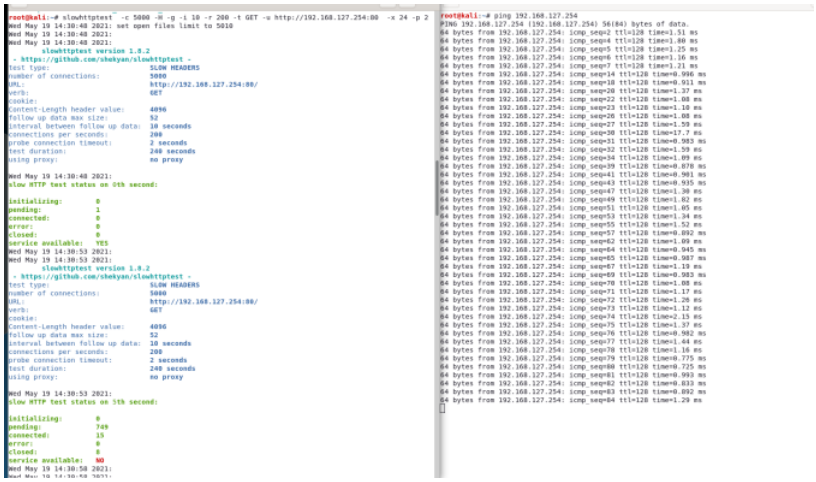
## 4GEE ROUTER HH70VB devices vulnerability

### Demonstration

Normally, MOXA Mgate MB3180 ‘s web login screenshot is like this. As shown below:




By using slowhttptest tool to attack to MOXA Mgate MB3180 ‘s web server, keep it waiting for response until its resource exhausted, therefore achieves Slow HTTP DoS Attack. If attack cause web server out of service successful ly, option service available will show text NO with red color. As shown below:



It could not be accessed when attack success. As shown below:


### Reference(s)

https://github.com/shekyan/slowhttptest

https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3180-mb3280-mb3480-series

### Moxa Security advisory

https://www.moxa.com/en/support/product-support/security-advisory/mgate-mb3180-3280-3480-protocol-gateways-vulnerabilities