

CVE - 2020 - 5902

De Silva K.R.K.D

2023/11/04

INTRODUCTION

A critical security flaw called CVE-2020-5902 was found in the F5 Network BIG-IP advanced firewall manager (AFM) and BIG-IP application delivery controller (ADC) products. This flaw gives unauthorized users access to the system and the ability for unauthenticated attackers to run arbitrary code on susceptible systems, possibly remotely executing code. This vulnerability, which falls under the category of remote code execution, is caused by an issue with the configuration of the Traffic Management User Interface (TMUI) of the impacted products. A weakness in its implementation could be used by hostile actors to take control of the BIG-IP system, which is managed and configured through this interface.

Because of its critical impact and potential for exploitation, CVE-2020-5902 has drawn a lot of attention from the cybersecurity community. Organizations utilizing the impacted products were advised to install the patches as soon as possible to reduce risk and safeguard their systems. F5 Networks released updates to address this vulnerability.

Table Of Content

INTRODUCTION 2

Exploitation Steps 4

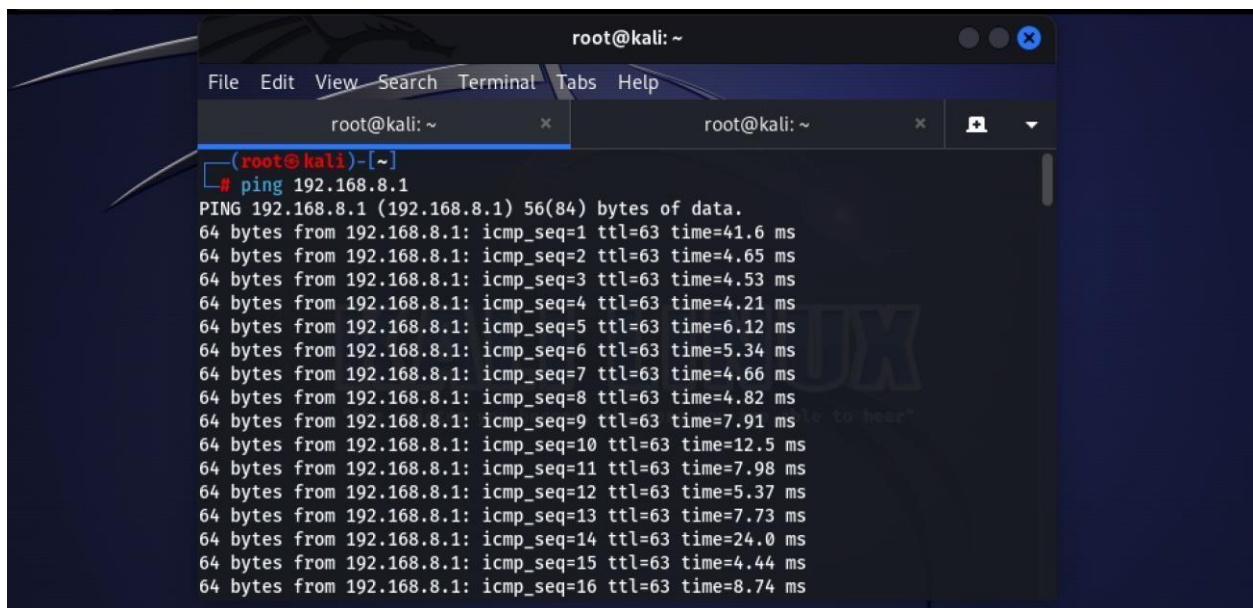
How To Mitigate 9

CONCLUSION..... 9

REFERENCES 9

Exploitation Steps

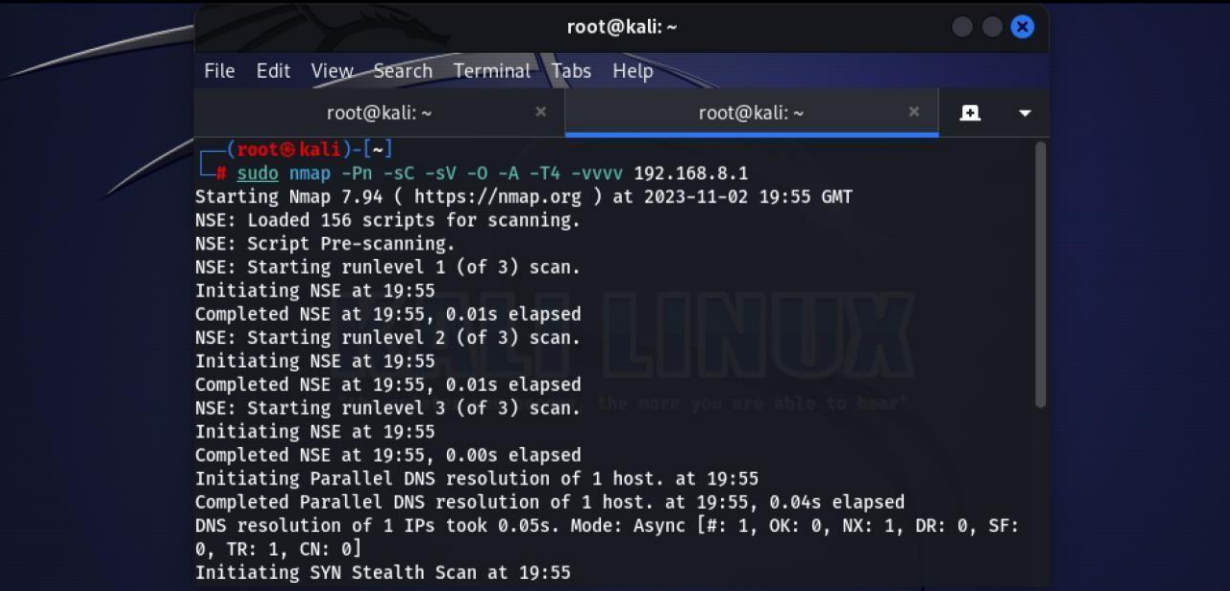
I used an IP address to exploit this vulnerability. First, I used “ping” command. This command is a useful network tool that determines how reachable a host or network device is over an IP network and how long it takes for data packets to travel back and forth from their source. Numerous operating systems, including Linux, Windows, and others, are compatible with it. This tool is commonly used for network diagnostics. It helps to confirm host responsiveness and assess network performance by measuring data packet round-trip times. It functions as a vital tool for network monitoring and troubleshooting.

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', 'Tabs', and 'Help'. Below the menu bar, there are two tabs, both labeled 'root@kali: ~'. The terminal content shows a user prompt '(root@kali)-[~]' followed by the command '# ping 192.168.8.1'. The output of the ping command is displayed, showing 16 successful pings to 192.168.8.1. Each line of output includes the IP address, sequence number, TTL, and round-trip time in milliseconds. The times vary, with most being between 4.21 ms and 7.98 ms, and one outlier at 24.0 ms for sequence 14. The terminal background is dark with light-colored text.

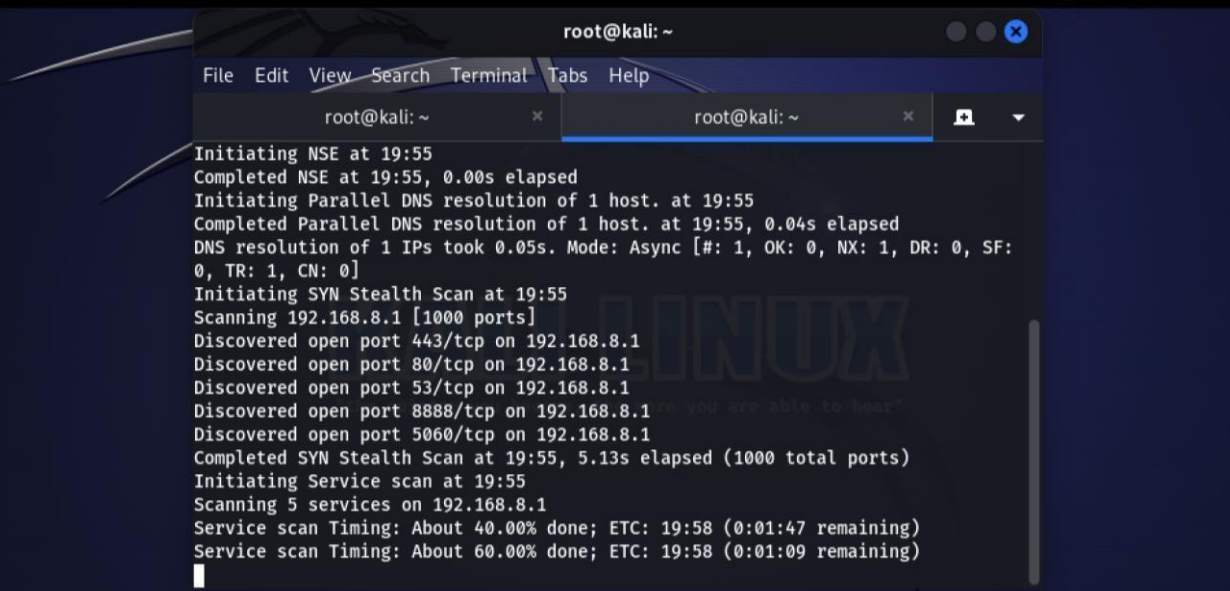
```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
(root@kali)-[~]
# ping 192.168.8.1
PING 192.168.8.1 (192.168.8.1) 56(84) bytes of data.
64 bytes from 192.168.8.1: icmp_seq=1 ttl=63 time=41.6 ms
64 bytes from 192.168.8.1: icmp_seq=2 ttl=63 time=4.65 ms
64 bytes from 192.168.8.1: icmp_seq=3 ttl=63 time=4.53 ms
64 bytes from 192.168.8.1: icmp_seq=4 ttl=63 time=4.21 ms
64 bytes from 192.168.8.1: icmp_seq=5 ttl=63 time=6.12 ms
64 bytes from 192.168.8.1: icmp_seq=6 ttl=63 time=5.34 ms
64 bytes from 192.168.8.1: icmp_seq=7 ttl=63 time=4.66 ms
64 bytes from 192.168.8.1: icmp_seq=8 ttl=63 time=4.82 ms
64 bytes from 192.168.8.1: icmp_seq=9 ttl=63 time=7.91 ms
64 bytes from 192.168.8.1: icmp_seq=10 ttl=63 time=12.5 ms
64 bytes from 192.168.8.1: icmp_seq=11 ttl=63 time=7.98 ms
64 bytes from 192.168.8.1: icmp_seq=12 ttl=63 time=5.37 ms
64 bytes from 192.168.8.1: icmp_seq=13 ttl=63 time=7.73 ms
64 bytes from 192.168.8.1: icmp_seq=14 ttl=63 time=24.0 ms
64 bytes from 192.168.8.1: icmp_seq=15 ttl=63 time=4.44 ms
64 bytes from 192.168.8.1: icmp_seq=16 ttl=63 time=8.74 ms
```

Then, I scanned that IP address using “sudo nmap -Pn -sC -sV -O -A -T4 -vvvv <ip>”. This command executes a comprehensive and aggressive scan of the target host without first confirming the host’s reachability. It wants to determine the operating system, find open ports and services, and run different NSE scripts for more data gathering and vulnerability analysis. Using such aggressive scans

responsibly is essential because they can be more noticeable and generate a significant amount of network traffic. When performing network scans.



```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x  
(root@kali)~[~]  
# sudo nmap -Pn -sC -sV -O -A -T4 -vvvv 192.168.8.1  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-02 19:55 GMT  
NSE: Loaded 156 scripts for scanning.  
NSE: Script Pre-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 19:55  
Completed NSE at 19:55, 0.01s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 19:55  
Completed NSE at 19:55, 0.01s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 19:55  
Completed NSE at 19:55, 0.00s elapsed  
Initiating Parallel DNS resolution of 1 host. at 19:55  
Completed Parallel DNS resolution of 1 host. at 19:55, 0.04s elapsed  
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF:  
0, TR: 1, CN: 0]  
Initiating SYN Stealth Scan at 19:55
```



```
Initiating NSE at 19:55  
Completed NSE at 19:55, 0.00s elapsed  
Initiating Parallel DNS resolution of 1 host. at 19:55  
Completed Parallel DNS resolution of 1 host. at 19:55, 0.04s elapsed  
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF:  
0, TR: 1, CN: 0]  
Initiating SYN Stealth Scan at 19:55  
Scanning 192.168.8.1 [1000 ports]  
Discovered open port 443/tcp on 192.168.8.1  
Discovered open port 80/tcp on 192.168.8.1  
Discovered open port 53/tcp on 192.168.8.1  
Discovered open port 8888/tcp on 192.168.8.1  
Discovered open port 5060/tcp on 192.168.8.1  
Completed SYN Stealth Scan at 19:55, 5.13s elapsed (1000 total ports)  
Initiating Service scan at 19:55  
Scanning 5 services on 192.168.8.1  
Service scan Timing: About 40.00% done; ETC: 19:58 (0:01:47 remaining)  
Service scan Timing: About 60.00% done; ETC: 19:58 (0:01:09 remaining)  
█
```

```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ root@kali: ~  
Initiating Service scan at 19:55  
Scanning 5 services on 192.168.8.1  
Service scan Timing: About 40.00% done; ETC: 19:58 (0:01:47 remaining)  
Service scan Timing: About 60.00% done; ETC: 19:58 (0:01:09 remaining)  
Completed Service scan at 19:58, 156.46s elapsed (5 services on 1 host)  
Initiating OS detection (try #1) against 192.168.8.1  
Retrying OS detection (try #2) against 192.168.8.1  
Initiating Traceroute at 19:58  
Completed Traceroute at 19:58, 0.03s elapsed  
Initiating Parallel DNS resolution of 2 hosts. at 19:58  
Completed Parallel DNS resolution of 2 hosts. at 19:58, 0.01s elapsed  
DNS resolution of 2 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 2, DR: 0, SF: 0, TR: 2, CN: 0]  
NSE: Script scanning 192.168.8.1.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 19:58  
Completed NSE at 19:58, 13.89s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 19:58  
Completed NSE at 19:58, 2.01s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 19:58  
Completed NSE at 19:58, 0.00s elapsed  
Nmap scan report for 192.168.8.1  
Host is up, received user-set (0.0062s latency).
```

```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ root@kali: ~  
| dns-nsid:  
|_ bind.version: dnsmasq-2.80  
80/tcp open http syn-ack ttl 64 Sanechips-Webs  
|_http-favicon: Unknown favicon MD5: A07E0861BD1BF8DC1B577C31A04DA957  
|_http-title: Site doesn't have a title (text/html).  
|_Requested resource was http://192.168.8.1/main.html  
|_http-trane-info: Problem with XML parsing of /evox/about  
|_http-server-header: Sanechips-Webs  
| fingerprint-strings:  
|_ HTTPOptions:  
|_ HTTP/1.1 400 Page not found  
|_ Server: Sanechips-Webs  
|_ X-Frame-Options: SAMEORIGIN  
|_ X-Content-Type-Options: nosniff  
|_ X-XSS-Protection: 1  
|_ Content-Expires: 0  
|_ Cache-control: no-store  
|_ Server: Sanechips-Webs  
|_ Date: Fri Nov 3 01:25:48 2023  
|_ X-Frame-Options: SAMEORIGIN  
|_ Pragma: no-cache  
|_ Cache-Control: no-store  
|_ Content-Type: text/html  
|_ <html><head><title>Document Error: Page not found</title></head>
```

```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x  
Pragma: no-cache  
Cache-Control: no-store  
Content-Type: text/html  
<html><head><title>Document Error: Page not found</title></head>  
<body><h2>Access Error: Page not found</h2>  
<p>Bad request type</p></body></html>  
Help:  
HTTP/1.1 400 Page not found  
Server: Sanechips-Webs  
X-Frame-Options: SAMEORIGIN  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1  
Content-Expires: 0  
Cache-control: no-store  
Server: Sanechips-Webs  
Date: Fri Nov 3 01:26:20 2023  
X-Frame-Options: SAMEORIGIN  
Pragma: no-cache  
Cache-Control: no-store  
Content-Type: text/html  
<html><head><title>Document Error: Page not found</title></head>  
<body><h2>Access Error: Page not found</h2>  
<p>Bad request type</p></body></html>  
RTSPRequest:
```

```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ x root@kali: ~ x  
HTTP/1.1 400 Page not found  
Server: Sanechips-Webs  
X-Frame-Options: SAMEORIGIN  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1  
Content-Expires: 0  
Cache-control: no-store  
Server: Sanechips-Webs  
Date: Fri Nov 3 01:25:49 2023  
X-Frame-Options: SAMEORIGIN  
Pragma: no-cache  
Cache-Control: no-store  
Content-Type: text/html  
<html><head><title>Document Error: Page not found</title></head>  
<body><h2>Access Error: Page not found</h2>  
<p>Bad request type</p></body></html>  
SSLSessionReq:  
HTTP/1.1 400 Page not found  
Server: Sanechips-Webs  
X-Frame-Options: SAMEORIGIN  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1  
Content-Expires: 0  
Cache-control: no-store
```



```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ root@kali: ~  
Bad request type<p></body></html>  
_ http-methods:  
_ Supported Methods: GET HEAD  
443/tcp open ssl/https? syn-ack ttl 64  
_ http-title: Site doesn't have a title (text/html).  
_ Requested resource was https://192.168.8.1/main.html  
_ http-methods:  
_ Supported Methods: GET HEAD  
_ http-favicon: Unknown favicon MD5: A07E0861BD1BFBD18577C31A04DA957  
_ ssl-cert: Subject: organizationName=tz/stateOrProvinceName=gd/countryName=cn/localityName=sz/organizationalUnitName=tz  
_ Issuer: organizationName=tz/stateOrProvinceName=gd/countryName=cn/localityName=sz/organizationalUnitName=tz  
_ Public Key type: rsa  
_ Public Key bits: 1024  
_ Signature Algorithm: sha256WithRSAEncryption  
_ Not valid before: 2018-07-03T06:49:39  
_ Not valid after: 2028-06-30T06:49:39  
_ MD5: d4a0:6190:3f89:d5e6:3806:d939:9354:6b69  
_ SHA-1: 27c8:e4fb:e811:a585:9778:f7b0:9f7e:5102:2da8:e87a  
_ -----BEGIN CERTIFICATE-----  
_ MITCTCCAX6gAwIBAgIJAPDSTrM97hMnMA0GCSqGSIb3DQEBCwUAMEEExCzAJBgNV  
_ BAYTAmNuMQswCQYDVQIDAJnZDELMAkGA1UEBwwCc3oxCzAJBgNVBAoMANR6MQsw  
_ CQYDVQQQLDAJ0ejaeFw0xODA3MDMwNjQ5MzlaFw0yODA2MzAwNjQ5MzlaMEExCzAJ  
_ BgNVBAYTAmNuMQswCQYDVQIDAJnZDELMAkGA1UEBwwCc3oxCzAJBgNVBAoMANR6  
_ MQswCQYDVQQQLDAJ0ejaeFw0xODA3MDMwNjQ5MzlaFw0yODA2MzAwNjQ5MzlaMEExCzAJ
```

```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~ root@kali: ~  
No exact OS matches for host (test conditions non-ideal).  
TCP/IP fingerprint:  
SCAN(V=7.94%E=4%D=11/2%OT=53%CT=%CU=Y%DS=2%DC=T%G=N%TM=6543FF75%P=x86_64-pc-linux-gnu)  
SEQ(SP=11%GCD=FA00%ISR=9C%TI=I%II=I%SS=S%TS=U)  
SEQ(SP=11%GCD=FA00%ISR=9C%TI=I%II=I%SS=S%TS=U)  
OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)  
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)  
ECN(R=Y%DF=N%TG=40%W=FFFF%O=M5B4%CC=N%Q=)  
T1(R=Y%DF=N%TG=40%S=O%A=S+F=AS%RD=0%Q=)  
T2(R=Y%DF=N%TG=FF%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)  
T3(R=Y%DF=N%TG=FF%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)  
T4(R=Y%DF=N%TG=FF%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)  
T5(R=Y%DF=N%TG=FF%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)  
T6(R=Y%DF=N%TG=FF%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)  
T7(R=Y%DF=N%TG=FF%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)  
U1(R=N)  
IE(R=Y%DFI=N%TG=40%CD=Z)  
  
Network Distance: 2 hops  
TCP Sequence Prediction: Difficulty=17 (Good luck!)  
IP ID Sequence Generation: Incremental  
  
TRACEROUTE (using port 443/tcp)  
0.0.0.0 -> 192.168.8.1
```

As a result, I got this IP's ports and attempted to detect the OS and run various NSE scripts.

How to mitigate

- Install a fixed software version.
- By limiting access to all TMUI interfaces and utilizing the mitigation procedures listed below for self Ips and the management interface, the risk can be reduced. [1]

CONCLUSION

In conclusion, F5 Networks' BIG-IP and advanced firewall manager products are susceptible to a critical vulnerability known as CVE-2020-5902. Network security is seriously threatened by this vulnerability, which could enable unauthorized attackers to run arbitrary code on impacted systems. The vulnerability can allow malevolent actors to access susceptible systems and insert malicious code, even when MFA is enabled. Even though more recent FortiGate versions may reject some requests, the potential consequences of this vulnerability make it a serious worry. Patching and mitigating this security risk immediately is essential to securing vulnerable systems.

References

- [1] "MyF5 (TMUI RCE vulnerability CVE-2020-5902)," 1 July 2020. [Online]. Available: <https://my.f5.com/manage/s/article/K52145254>.