Security Advisory

AI Recommended Content

K52145254: TMUI RCE vulnerability CVE-2020-5902

Published Date: **Jul 1, 2020** Updated Date: **Feb 21, 2023**

Evaluated products:

Final- This article is marked as 'Final' because the security issue described in this article either affected F5 products at one time and was resolved or it never affected F5 products. Unless new information is discovered, F5 will no longer update the article.

Security Advisory Description

`The Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.` (CVE-2020-5902)

Impact

This vulnerability allows for unauthenticated attackers, or authenticated users, with network access to the Configuration utility, through the BIG-IP management port and/or self IPs, to execute arbitrary system commands, create or delete files, disable services, and/or execute arbitrary Java code. This vulnerability may result in complete system compromise. The BIG-IP s plane; only the control plane is affected.

***Note**: All information present on an infiltrate logs, configurations, credentials, and digital certificates.*

Important: If your BIG-IP system has TMU there is a high probability that it has been compromised and you should follow se section.

We value your privacy

To provide the best experience, we leverage third-party technologies to personalize what you see, and to better understand what content is important to you. View our privacy policy for details.

Customize Settings No thanks Count me in

Security Advisory Status

F5 Product Development has assigned IDs

To determine if your product and version h box. To determine if your release is known to be vulnerable, the components or features that are affected by the vulnerability, and for information about releases, point releases, or hotfixes that address the vulnerability, refer to the following table. For more information about security advisory versioning, refer to K51812227: Understanding Security Advisory versioning.

Product	Branch	Versions known to be vulnerable	Fixes introduced in	Severity	CVSSv3 score[1]	Vulnerable component or feature
BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO, CGNAT)	16.x	None	16.0.0	Critical	10.0	TMUI/Configuration utility
	15.x	15.1.0 15.0.0 - 15.0.1	15.1.0.4[‡] 15.0.1.4			
	14.x	14.1.0 - 14.1.2	14.1.2.6			
	13.x	13.1.0 - 13.1.3	13.1.3.4[†]			
	12.x	12.1.0 - 12.1.5	12.1.5.2			
	11.x	11.6.1 - 11.6.5	11.6.5.2			
BIG-IQ Centralized Management	7.x	None	Not applicable	Not vulnerable	None	None
	6.x	None	Not applicable			

	5.x	None	Not applicable			
Traffix SDC	5.x	None	Not applicable	Not vulnerable	None	None

[1] The CVSSv3 score link takes you to a resource outside of AskF5, and it is possible that the document may be removed without our knowledge.

*[†] An issue has been identified with the VIPRION B2250 blade and 13.1.3.4. Before installing this version on the B2250 blade, review: **K02251382: B2250 VIPRION Fails to boot After Upgrade to v13.1.3.4 installed.***

*[‡] An issue has been identified with some FIPS platforms (5250v-F, 7200v-F, 10200v-F, 10350v-F, i5820-DF, and i7820-DF) and 15.1.0.4. Before installing this version on these platforms, review: **K14635126: FIPS platforms fail to load configuration after upgrade to 15.1.0.4**.*

***Note**: Versions that have reached End of Technical support (EoTS) have not been evaluated but should be assumed vulnerable. For more information, refer to **K5903: BIG-IP software support policy**.*

Security Advisory Recommended Actions

If you are running a version listed in the **Versions known to be vulnerable** column, you can eliminate this vulnerability by installing a version listed in the **Fixes introduced in** column. If the table lists only an older version than what you are currently running, or does not list a non-vulnerable version, then no update candidate currently exists.

If you are using public cloud marketplaces (AWS, Azure, GCP, and Alibaba) to deploy BIG-IP Virtual Edition (VE), F5 recommends that you install the latest releases of BIG-IP versions listed in the **Fixes introduced in** column, subject to their availability on those marketplaces. See K84554955: Overview of BIG-IP systems software upgrades.

Mitigation

Important: F5 recommends that you insta

We value your privacy

To provide the best experience, we leverage third-party technologies to personalize what you see, and to better understand what content is important to you. View our privacy policy for details.

If it is not possible to update quickly, you ca s complete:

- Restrict Access:
  - Self IPs: addresses unauthenticated
  - Management interface: addresses
- TMUI httpd: addresses unauthenticated
  - Command line
  - iControl REST

Important: F5 strongly recommends insta may be mitigated by restricting access to all TMUI interfaces using the following mitigation steps provided for self IPs and the management interface.

Restrict Access

Self IPs

You can block all access to the Configuration utility of your BIG-IP system using self IPs. To do so, you can change the **Port Lockdown** setting to **Allow None** for each self IP in the system. If you must open any ports, you should use the **Allow Custom** option, taking care to disallow access to the Configuration utility. By default, the Configuration utility listens on TCP port 443; however, beginning in BIG-IP 13.0.0, Single-NIC BIG-IP VE deployments use TCP port 8443. Alternatively, you can configure a custom port.

***Note**: Performing this action prevents all access to the Configuration utility using the self IP. These changes may also impact other services, including breaking HA configurations.*

Before you make changes to the configuration of your self IPs, F5 strongly recommends that you refer to the following articles:

- K17333: Overview of port lockdown behavior (12.x - 16.x)
- K13092: Overview of securing access to the BIG-IP system
- K31003634: The Configuration utility of the Single-NIC BIG-IP Virtual Edition now defaults to TCP port 8443
- K51358480: The single-NIC BIG-IP VE may erroneously revert to the default management httpd port after a configuration reload

Management interface

To mitigate this vulnerability for affected F5 products, you should permit management access to F5 products only over a secure network. For more information about securing access to BIG-IP systems, refer to K13309: Restricting access to the Configuration utility by source IP address (11.x - 16.x) and K13092: Overview of securing access to the BIG-IP system.

***Note**: Until a fixed release is installed, authenticated users accessing the Configuration utility will always be able to exploit this vulnerability.*

TMUI httpd

Important: This section was last updated on July 8, 2020 at 17:00 Pacific time.

The mitigation provided below is based on the information available to F5 at this time. It may not be a complete mitigation. However, F5 feels this information is useful to our customers as it mitigates the unauthenticated exploits currently known to us. As F5 becomes aware of any future variants, we will continue to update this article.

To prevent unauthenticated attackers from exploiting this vulnerability, add a **LocationMatch** configuration element to **httpd**. To do so, perform the following procedure:

***Note**: Authenticated users will still be able to exploit the vulnerability, independent of their privilege level.*

***Impact of workaround**: The following mitigation adds an include statement to the **httpd** properties. If your **httpd** properties contain an existing include statement (the include statement is something other than the default of none), you need to prepend/append your existing included configuration to the changes, or it will be overwritten. For example, if your existing include statement is:*

```
include "FileETag MTime Size"
```

Then you can append the LocationMatch statement in the mitigation to the existing configuration as follows:

```
include 'FileETag MTime Size
<LocationMatch ";">
Redirect 404 /
</LocationMatch>
<LocationMatch "hsqldb">
Redirect 404 /
</LocationMatch>
'
```

You can perform the mitigation locally using the command line or remotely using the iControl REST interface.

Command line

1. Log in to the TMOS Shell (**tms**

```
tmsh
```

2. Edit the **httpd** properties by e

```
edit /sys httpd all-pr
```

***Note**: Running this command*

3. Locate the line that starts with

```
include '
        <LocationMatch
        Redirect 404 /
        </LocationMatch>
        <LocationMatch "hsqldb">
        Redirect 404 /
        </LocationMatch>
        '
```

4. Write and save the changes to the configuration file by entering the following **vi** commands:

```
Esc
        :wq!
```

5. When further prompted to **Save Changes (y/n/e)**, enter **y**.
6. Save the configuration by entering the following **tmsh** command:

```
save /sys config
```

7. To activate the mitigation, restart the **httpd** service by entering the following command:

```
restart sys service httpd
```

8. To exit **tmsh**, enter the following command:

```
quit
```

9. Ensure that the workaround is inserted in the configuration by comparing the output of the following command to the configured **LocationMatch** fragment that you inserted in **step 3**. To do so, enter the following command:

```
grep -C1 'Redirect 404' /etc/httpd/conf/httpd.conf
```

The output should match the following:

```
<LocationMatch ";">
Redirect 404 /
</LocationMatch>
<LocationMatch "hsqldb">
```

```
Redirect 404 /
</LocationMatch>
```

***Note**: You may disregard any leading white spaces.*

10. If you have a high availability (HA) configuration, you may now perform a **ConfigSync** operation as documented in K14856: Performing a ConfigSync using tmsh. No restart of **httpd** on the peer system should be required after syncing. Confirm the mitigation is working using the following instructions.

    iControl REST

    ```
    # Patch the httpd configuration
    curl -ku admin:[password] https://[IP Address]/mgmt/tm/sys/httpd -H content-type:application/json -X PATCH -d
    '{"include":"\n <LocationMatch \\\";\\\">\n Redirect 404 /\n </LocationMatch>\n <LocationMatch \\\"hsqldb\\\">\n
    Redirect 404 /\n </LocationMatch>\n "}' | jq .

    # Save the system config
    curl -ku admin:[password] https://[IP Address]/mgmt/tm/sys/config -H "Content-Type: application/json" -X POST -d
    '{"command":"save"}' | jq .

    # Verify the configuration
    curl -ku admin:[password] https://[IP Address]/mgmt/tm/sys/httpd -H "Content-Type: application/json" -X GET | jq .
    ```

    If you have an HA configuration, you may also synchronize these changes with the peers:

    ```
    curl -ku admin:[password] https://[IP Address]/mgmt/tm/cm -H "Content-Type: application/json" -X POST -d
    '{"command":"run","utilCmdArgs":"config-sync to-group [Device Group Name]"}' | jq .
    ```

    No restart of **httpd** on the peer should be required after syncing. Confirm the mitigation is working using the following instructions.

    ***Note**: Running REST commands in rapid succession may cause issues. F5 advises that you allow time for completion between commands.*

    ***Note**: This mitigation previously included a step to restart **httpd**. It has been determined that the restart is not required when using REST. Furthermore, the restart command may cause is* *sing the iControl REST API.*

    ***Note**: F5 is aware of customer* *nended mitigation above. This has not been an effective mitigation and dev*

Verifying the mitigation

You can verify that the mitigation is working

- `https://[IP ADDRESS]/tmui/log`
- `https://[IP ADDRESS]/hsqldb%0`

We value your privacy

To provide the best experience, we leverage third-party technologies to personalize what you see, and to better understand what content is important to you. View our privacy policy for details.

Before applying the mitigation, the pages load. After the mitigation, you receive **404** responses.

Note: In fixed versions you will receive a 302 Redirect response directing you to the login page.

Indicators of compromise

Important: This section was last updated on July 20, 2020 at 20:00 Pacific time.

This information is based on the evidence F5 has seen on compromised devices, which we feel are reliable indicators. It is important to note that not all exploited systems may show the same indicators, and, indeed, a skilled attacker may be able to remove traces of their work. It is not possible to prove a device has not been compromised; when there is any uncertainty, you should consider the device compromised.

All versions

F5 iHealth is updated with heuristics which flag indicators of compromise in uploaded QKView diagnostic files. Refer to K27404821: Using F5 iHealth to diagnose vulnerabilities for more information on using F5 iHealth. Through the DevCentral GitHub, F5 has also released the CVE-2020-5902 IoC Detection Tool. This is a Python script designed to run on the command line to locally identify indicators of compromise.

If you are unable to use the CVE-2020-5902 IoC Detection Tool, you may also perform some of the following checks manually:

- Look for the creation of aliases for the Advanced Shell (**bash**); the presence of an alias is a strong indicator of a potential compromise. To do so, run the following command:

  ```
  awk '/^cli.alias/,/^}/' /config/bigip_*.conf
  ```

  You may observe results similar to the following:

  ```
  cli alias private list {
      command bash
      user root
  }
  ```

If you see results similar to this, it is a possible indicator of compromise. You should determine if the result is legitimate for your configuration.

- Check for user 'systems' in **/config/bigip_user.conf** and **/etc/passwd**; several exploits have created this non-standard user. To do so, run the following commands:
  ```
  awk '/systems/' /config/bigip_user.conf
  grep -i 'systems' /etc/passwd
  ```
- Examine **/var/log/audit** for common patterns seen with exploits. To do so, run the following command:
  ```
  zgrep -e "create cli alias" -e "run /util bash /tmp" -e "list auth user admin" -e "_alias" -e "create auth user" -e "load user credentials for user" /var/log/audit*
  ```

  You may see a result similar to the following:

  ```
  Jul 14 12:59:57 [REDACTED] notice tmsh[13316]: 01420002:5: AUDIT - pid=13316 user=root folder=/Common module=(tmos)# status=[Command OK] cmd_data=create cli alias private list command bash
  ```
  If this command returns a similar result, it may be a possible indicator of compromise. You need to examine the results to determine if you can account for them due to legitimate activity.
- Check for files created in **/usr/local/www/** since the CVE announcement. It is common for exploit scripts to create files in this directory. If you find any files, determine if they can be accounted for from legitimate activity. If not, this is a strong indicator of compromise. To check files, run the following command:
  ```
  touch -t 202006290100 /tmp/kbtime; find /usr/local/www/ -type f -newer /tmp/kbtime -ls;
  ```

Additionally, refer to the following articles:

- K60058401: URI logging with HTTPD to audit requests sent to TMUI / GUI
- K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system for an overview

Versions prior to BIG-IP 14.1.0

In versions earlier than BIG-IP 14.1.0, with the default configuration, you can examine **/var/log/audit** and **/var/log/ltm** as follows. There is no supported mechanism to expose additional log entries.

To examine the logs, use the following command:

```
zgrep '%tmui' /var/log/audit* /var/log/ltm*
```

Log entries similar to the following are indic

```
audit.1:Jul  6 15:33:38 [REDACTED]                                            ntials for user "%tmui" Current
session has been terminated.
ltm.1:Jul  6 15:33:38 [REDACTED] r                                             user "%tmui" Current session has
been terminated.
```

BIG-IP 14.1.0 and later

In BIG-IP 14.1.0 and later, you can examine t   ring the following command in **bash**:

```
journalctl /bin/logger | grep -F
```

The command output may appear similar to the following example on a device where compromise was attempted; note that some elements are redacted (normally the complete URL is visible, along with the IP address that sent the request):

```
Jul 06 12:59:01 hostname logger[29929]: [ssl_acc] nnn.nnn.nnn.nnn - - [06/Jul/2020:12:59:01 +0000] "/[REDACTED]/..;/[REDACTED]" 200 252
```

If any log entries are shown, this may be an indicator of an attempt to compromise the BIG-IP system. Take specific note of the second to last value in the line, in this case **200**; the HTTP Response Code. A **200** indicates that the request was successful, which is a strong indicator of a successful exploit. A **404** response code means the requested item was not found. This may be a sign of an attempted compromise or a scanner being run against the device. You may also see **404** requests logged on devices using mitigation or which are running fixed software. The requests are still being made, but they are unsuccessful.

***Note**: Journal log entries are rotating and limited to ~20 MB and therefore may contain limited historical information.*

***Note**: These log entries are only created by unauthenticated attacks. Authenticated attackers do not leave this record behind.*

Other indicators of compromise may include unexpected modifications to any files, configurations, or running processes. F5 has iHealth heuristics designed to detect unknown processes running (Heuristic H511618) and also heuristics designed to detect when the Configuration utility has been exposed to the Internet through the management interface (H444724) or when a self IP address has **Port Lockdown** set to **Allow All** (H458565).

***Note**: Lack of log entries or heuristic reports do not categorically indicate that a unit has not been compromised. A skilled attacker can remove evidence of compromise, including log files, following successful exploitation.*

Acknowledgements

F5 would like to acknowledge Mikhail Klyuchnikov of Positive Technologies for bringing this issue to our attention and for following the highest standards of coordinated disclosure.

F5 would like to acknowledge Rich Mirch, Senior Adversarial Engineer, and Chase Dardaman, Senior Adversarial Engineer, from TeamARES of Critical Start, Inc. for bringing an issue with the original mitigation to our attention and for following the highest standards of coordinated disclosure.

Related Content

- K41942608: Overview of Security Advisory articles
- K4602: Overview of the F5 security vulnerability response policy
- K4918: Overview of the F5 critical issue hotfix policy
- K9502: BIG-IP hotfix and point release matrix
- K84554955: Overview of BIG-IP systems software upgrades
- K13123: Managing BIG-IP product hotfixes (11.x - 16.x)
- K167: Downloading software and firmware from F5
- K9970: Subscribing to email notifications regarding F5 products
- K9957: Creating a custom RSS feed to view new and updated documents
- K46122561: Restricting access to the management port using network firewall rules
- K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system
- DevCentral: Traffic Management User Interface Vulnerability: How to mitigate

AI Recommended Content

- Security Advisory - K000148343: Diffie-Hellman key exchange protocol vulnerability CVE-2024-41996
- Knowledge - K000135931: Contact F5 Support
- Security Advisory - K000148314: MySQL vulnerabilities CVE-2024-21232 and CVE-2024-21212
- Security Advisory - K000148313: MySQL vulnerabilities CVE-2024-21247, CVE-2024-21209, and CVE-2024-21231

Return to Top

* Was this information helpful?

○ Yes ○ No

How can we improve this content?

May we contact you directly regardi

○ Yes ○ No

We value your privacy

To provide the best experience, we leverage third-party technologies to personalize what you see, and to better understand what content is important to you. View our privacy policy for details.

Contact Support

HAVE A QUESTION? | Support and Sales ›

FOLLOW US

ABOUT F5
Corporate Information
Newsroom
Investor Relations
Careers
Contact Information
Communication Preferences

EDUCATION
Training
Certification
LearnF5
Free Online Training

F5 SITES
F5.com
DevCentral
MyF5
Partner Central
F5 Labs

SUPPORT TASKS
Read Support Policies
Create Support Case
Leave Feedback [+]