Ebode摄像头（foscam OEM）安全分析

# 漏洞挖掘流程简述

通过分析该摄像头需要先通过有线网络连接进入WLAN，后可以设置Wireless链接对其进行无线控制。首先我们对该产品进行调查，在配置IP后，访问该摄像头的Web管理端后通过抓取到了此链接：  
<http://100.84.124.183/get_params.cgi>

A screenshot of a cell phone

Description automatically generated

固件版本

通过谷歌搜索引擎，搜索到了以下内容。

A screenshot of a cell phone

Description automatically generated

版本号

该产品的固件版本与一款名为foscam的摄像头使用同一系列的固件。通过翻阅foscam官方网站的文档，

<https://www.foscam.es/descarga/ipcam_cgi_sdk.pdf>

A screenshot of a cell phone

Description automatically generated

通过阅读文档发现该设备软件以x.x.2.41形式进行版本号的管理。

A screenshot of a cell phone

Description automatically generated

于是在官网上可以下载到对应的固件，

[fi8906w\_firmware\_11.35.2.49\_fr\_chipset\_.zip](http://www.foscam.eu/index.php/productattachments/index/download?id=129)

通过使用以下命令，

% hexdump lr\_cmos\_11\_35\_2\_49.bin|less

可以发现该文件的第二行第四个字节是‘50 4b 03 04 ’ 对应的ascii 字符为PK，该字符为压缩文件的Magic Number，所以通过dd命令获取该文件的zip文件内容。

以下为Zip文件格式：

**End of central directory record:**

Offset   Length   Contents

  0      4 bytes  End of central dir signature (0x06054b50)

  4      2 bytes  Number of this disk

  6      2 bytes  Number of the disk with the start of the central directory

  8      2 bytes  Total number of entries in the central dir on this disk

 10      2 bytes  Total number of entries in the central dir

 12      4 bytes  Size of the central directory

 16      4 bytes  Offset of start of central directory with respect to the starting disk number

 20      2 bytes  zipfile comment length (c)

 22     (c)bytes  zipfile comment

dd if=lr\_cmos\_11\_35\_2\_49.bin of=test.zip  skip=0x14 count=764084 bs=1

可以通过该命令获取linux.bin文件。剩余的字节可以看出来是一个romfs文件系统

A close up of a computer

Description automatically generated

在挂载linux.bin后，将camera的bin文件（后端服务器）从目录中提取出来，通过查阅文档可以发现这是一个bflt文件格式的文件，

该文件格式是将linux中ELF的文件中的text段和data段抽取出来合成为一个新文件。

接下来对该camera的程序文件进行分析。IDA提供了解析bflt格式的python脚本，不过该脚本默认使用coolfire模式，需要修改一点脚本的内容，将其修改为摄像头使用的arm格式。

程序后端不是真实的cgi服务端，实际上后端使用了使用冗余的if循环判断文件它应该调用相应的哪个函数。

A screenshot of a social media post

Description automatically generated

通过分析固件的逆向代码结合对HTTP流量的审计，发现了以下漏洞。

攻击者无需认证即可访问以下链接：

<http://100.84.124.155/get_status.cgi>

该接口可以获取该摄像头的系统信息，例如系统固件版本号码等信息。

A screenshot of a cell phone

Description automatically generated

<http://100.84.124.155/decoder_control.cgi?command=1&next_url=/proc/kcore>

通过住个分析CGI接口，到第四个函数时，可以发现该接口可以读取任意文件，通过去读kcore可以获取内存中的所有信息，包含用户账户名和密码。

A close up of a newspaper

Description automatically generated

A picture containing appliance, cooling, window, white

Description automatically generated

A close up of a window

Description automatically generated

内存中的密码