

---

# 2023 攻防演习每日情报汇总

漏洞盒子

2023-8-15

演练第七天,红蓝队似乎已经有些疲惫,但随着新一批出局的消息被传出来,蓝队继续保持着高警惕状态;让我们一起看看今天又有那些资讯吧!

## 1、漏洞情报简讯

今日斗象漏洞情报中心通过情报星球社区捕获大量的 0day 漏洞,以下是今日捕获的 0day 漏洞及 nday 漏洞列表。

### 1.1 漏洞简讯

- **某 ecg-boot freemark 远程代码执行漏洞**: 漏洞等级严重, 确认 0day 漏洞, POC 小范围传播; 影响至最新版本。披露时间: 2023/8/15
- **某远 OA 存在文件上传漏洞**: 漏洞等级严重, 可能为 0day 漏洞, POC 小范围传播; 影响版本未知, 漏洞披露时间: 2023/8/15
- **某企互联 OA 登录绕过漏洞**: 漏洞等级高危, 可能为 0day 漏洞, POC 未公开; 影响版本未知, 漏洞披露时间: 2023/8/15
- **某恒明御安全网关远程命令执行漏洞**: 漏洞等级严重, 可能为 0day 漏洞, POC 小范围传播; 影响版本未知, 漏洞披露时间: 2023/8/15
- **某普前置服务管理平台远程命令执行漏洞**: 漏洞等级严重, 可能为 0day 漏

---

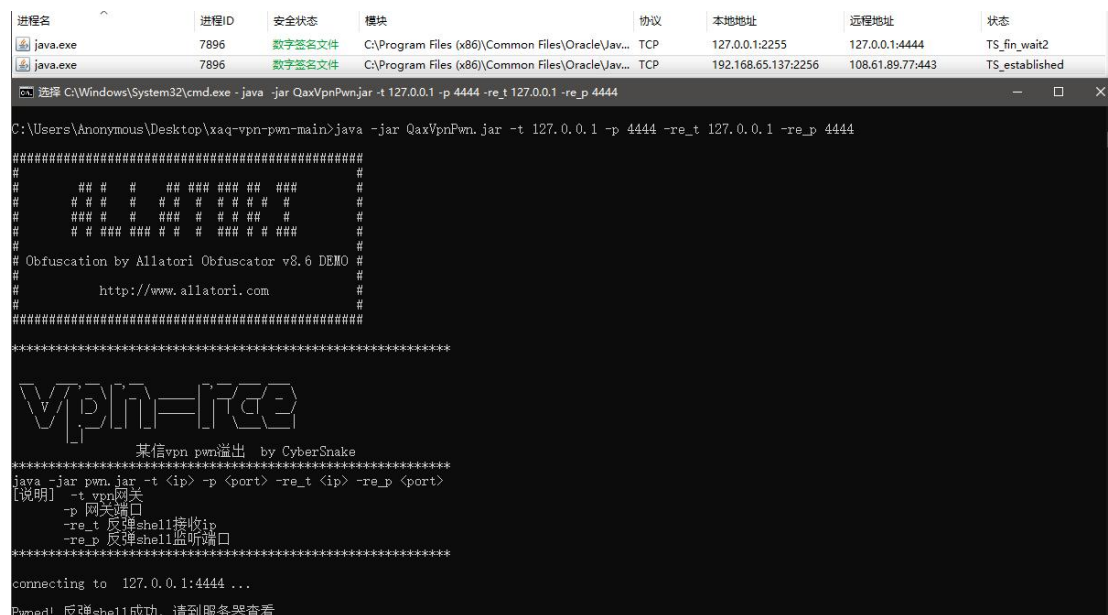
洞，POC 公开；影响版本未知，漏洞披露时间：2023/8/15

- **某蝶云星空任意文件读取漏洞**：漏洞等级严重，可能为 0day 漏洞，POC 公开；影响版本未知，漏洞披露时间：2023/8/15
- **某凌任意文件上传漏洞**：漏洞等级严重，可能为 0day 漏洞，POC 公开；影响版本未知，漏洞披露时间：2023/8/15
- **某远 OA M1Server 反序列化漏洞**：漏洞等级严重，可能为 0day 漏洞，POC 公开；影响版本未知，漏洞披露时间：2023/8/15

## 1.2 红队投毒案例精选

### ● 利用工具进行投毒

斗象情报中心侦测到红队投毒，样本 SHA256： d17983431d77228df214de758df87281bf7426a5eedbe673f25149c2f197c56b。



```
C:\Windows\System32\cmd.exe - java -jar QaxVpnPwn.jar -t 127.0.0.1 -p 4444 -re_t 127.0.0.1 -re_p 4444

C:\Users\Anonymous\Desktop\xaq-vpn-pwn-main>java -jar QaxVpnPwn.jar -t 127.0.0.1 -p 4444 -re_t 127.0.0.1 -re_p 4444

#####
#
#   # # # # # # # # # # # # # # # #
#   # # # # # # # # # # # # # # # #
#   # # # # # # # # # # # # # # # #
#   # # # # # # # # # # # # # # # #
#   # # # # # # # # # # # # # # # #
#
# Obfuscation by Allatori Obfuscator v8.6 DEMO
#
#   http://www.allatori.com
#
#####
*****
Vpn=Ice
某信vpn pwn溢出 by CyberSnake
*****
java -jar pwn.jar -t <ip> -p <port> -re_t <ip> -re_p <port>
【说明】
  -t vpn网关
  -p 网关端口
  -re_t 反弹shell接收ip
  -re_p 反弹shell监听端口
*****
connecting to 127.0.0.1:4444 ...
Pwned! 反弹shell成功, 请到服务器查看
```

外连可疑 IP：108.61.89.77

github 仓库：<https://github.com/CyberSnakeSec/xaq-vpn-pwn>

### ● 利用邮件进行钓鱼

斗象情报中心侦测到红队投毒，样本 SHA256： f9cc89ef84bfc6b9b39038635f8ed70999f2acef723428a1fcc4a764cfce9960。

外连 IP：123.57.247.152

邮件主题：XX 平台账号无法登录问题反馈

邮件发件人：18775800048@163.com

相关样本：**SoftServ.exe**(a2006fed8845bb8eefae6b0eca7fe179da5379f95e0fd09f8e64d6d809f48799)

情报来源: <https://planet.vulbox.com/detail/MTUwNzk=>

- 利用邮件进行钓鱼

斗象情报中心侦测到红队投毒, 样本 SHA256: 220f6b9f96106f637b339e2c6aee7259e76a9fd8a7237bc69ca7c1412bb8f992。2c6aee7259e76a9fd8a7237bc69ca7c1412bb8f992。



外连域名: static.windowsappupdate.com(104.21.38.87)

邮件主题: 【紧急】终端安全软件安装协助

邮件发件人: \*@dameng.org

相关样本: 火绒企业版终端.zip(8192f55ec81a355af642836cd39ebcaf14371822e06f5ee8dc8d64d658ad2dfc)、新建 ZIP 压缩文件.zip(cf34fd7f2d03572193098d48c55af6fa13fc6f5fe8244e976740dadf2c6883f4)

情报来源: <https://planet.vulbox.com/detail/MTQ5Njc=>

- 利用邮件进行钓鱼

斗象情报中心侦测到红队投毒, 样本 SHA256: 9a4f48d5da86819e5b53df2ed2bd82c393ddd3a944df2d26e14db025ff9855b3。2ed2bd82c393ddd3a944df2d26e14db025ff9855b3。

经检测该文件为高危文件

文件名称: wpsupdate.exe

SHA256: 9a4f48d5da86819e5b53df2ed2bd82c393ddd3a944df2d26e14db025ff9855b3

引擎检测结果: 

动态引擎分析1

动态引擎分析2

动态引擎分析3

静态特征检测

任务提交时间: 2023-08-15 19:29:46

最近检测时间: 2023-08-15 19:44:26

重新分析

样本下载

下载报告

收藏

分享

高危

① 分数说明

外连域名: cdn.windowsappupdate.com(104.21.38.87)

邮件主题: 【紧急】关于 WPSOffice 用户更新漏洞补丁的安全公告

邮件发件人: \*@dameng.org

情报来源: <https://planet.vulbox.com/detail/MTQ5Njc=>

## 2、 漏洞验证及复现

### 2.1 某 ecg-Boot 远程代码执行漏洞

系统未对用户输入内容进行过滤，导致未授权攻击者可以进行远程代码执行。

漏洞复现截图：



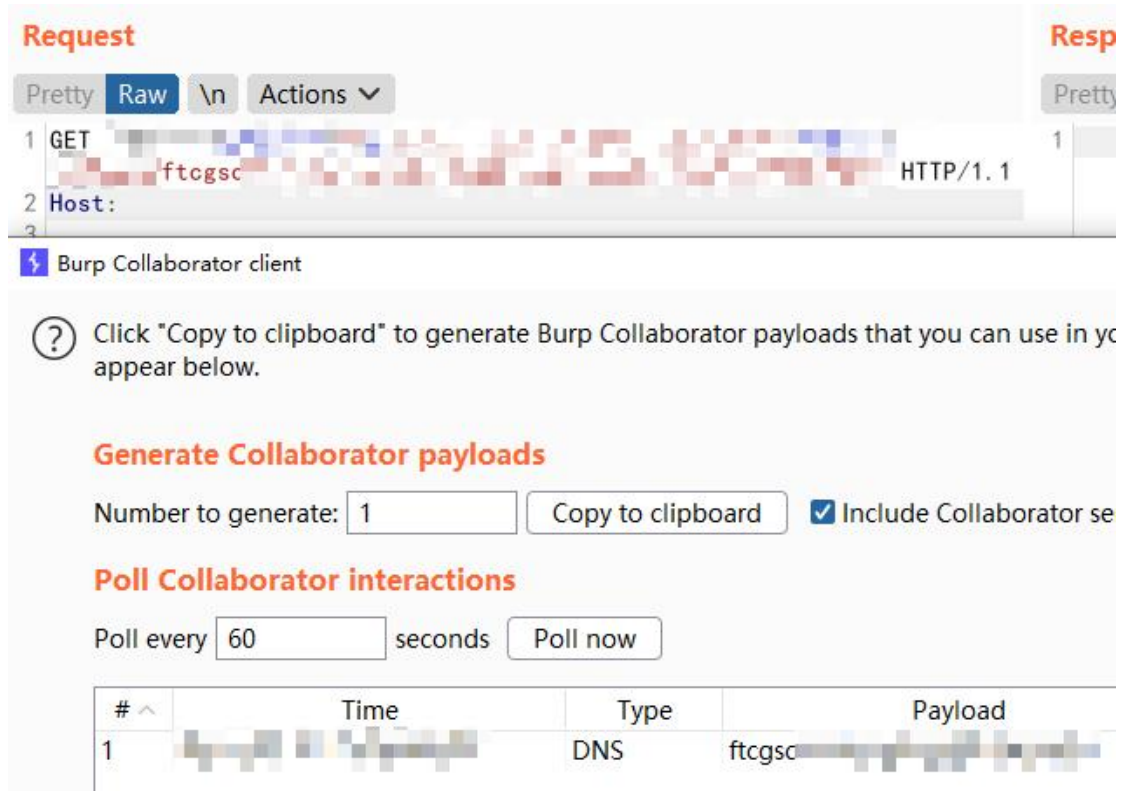
修复建议：

使用 WAF 设备对用户请求的关键字符进行过滤。

### 2.2 某恒明御安全网关 远程命令执行漏洞

系统未对用户输入内容进行过滤，导致未授权攻击者可以进行远程命令执行。

漏洞复现截图：



修复建议：

请使用该产品的用户尽快收缩资产，不要将其暴露在公网中；或使用 WAF 设备对请求进行过滤。

## 2.3 某远 OA M1Server 反序列化漏洞

系统未对用户输入内容进行过滤，导致反序列化触发远程代码执行利用。

漏洞复现截图：

**Request**

Pretty Raw \n Actions ▾

```
1 POST [redacted] HTTP/1.1
2 Host: [redacted]
3 Connection: close
4 Content-Length: 12740
5 Content-Type: application/x-www-form-urlencoded
6 cmd: whoami
7 Accept-Encoding: gzip, deflate
8
9 [redacted]
10
11 [redacted]
```

**Response**

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Date: Tue, 15 Aug 2023 12:05:57 GMT
4 Connection: close
5 Content-Length: 21
6
7 nt authority\system
8
```

**修复建议：**

使用 WAF 设备对用户输入的请求进行过滤。



---

### 3、 情报星球社区精选

我们看看今天情报星球社区都在热议什么：

1. 0day! jeecg-boot freemark 远程代码执行漏洞

<https://planet.vulbox.com/detail/MTUwOTI=>

本漏洞斗象情报中心已经复现验证，具体详情可参考以下链接：

<https://vip.tophant.com/detail/1691414640971616256>

2. 某工业集团有限公司共享威胁情报

<https://planet.vulbox.com/detail/MTUxNTU=>

3. 某远 OA 存在文件上传漏洞(疑似老洞 Bypass)

<https://planet.vulbox.com/detail/MTUxMzg=>

4. 某捷-EG 易网关组合拳 RCE

<https://planet.vulbox.com/detail/MTUxMzU=>

5. 某企互联 OA 登录绕过漏洞

<https://planet.vulbox.com/detail/MTUxOTA=>

『情报星球』是漏洞盒子平台旗下安全情报交流与分享社区。近期社区推出攻防演练情报奖励计划，欢迎参与：<https://activity.vulbox.com/awardPlan>

更多情报讨论与分享请访问『漏洞盒子-情报星球』：

<https://planet.vulbox.com>



扫码关注情报星球

手机看情报，把安全装进口袋

网络安全科技

## 4、疑似红队攻击 IP 汇总

斗象情报中心在攻防第七日捕获大量疑似红队攻击 IP 地址，蓝队可根据地址针对性设置防御策略：

时间	IP 地址	归属地
2023/8/15	185.225.75.242	保加利亚
2023/8/15	185.13.224.52	荷兰
2023/8/15	117.161.55.135	中国内蒙古呼和浩特市移动
2023/8/15	117.129.65.69	中国北京移动
2023/8/15	116.30.231.93	中国广东深圳市电信
2023/8/15	60.251.190.147	中国台湾中华电信(HiNet)数据中心
2023/8/15	61.141.31.3	中国广东汕头市电信
2023/8/15	61.129.103.137	中国上海浦东新区电信
2023/8/15	61.129.103.136	中国上海浦东新区电信
2023/8/15	61.129.103.135	中国上海浦东新区电信
2023/8/15	61.129.103.127	中国上海浦东新区电信
2023/8/15	61.1.239.173	印度
2023/8/15	61.130.136.39	中国浙江宁波市电信
2023/8/15	60.205.188.203	中国北京阿里云 BGP 服务器
2023/8/15	60.205.168.102	中国北京阿里云 BGP 服务器
2023/8/15	60.188.9.84	中国浙江台州市黄岩区电信
2023/8/15	60.167.27.42	中国安徽芜湖市电信

---

2023/8/15	59.98.125.111	印度 BSNL 网络
2023/8/15	59.8.33.146	韩国 KT 电信
2023/8/15	59.178.75.129	印度 VSNL 网络

更多疑似红队攻击 IP 请参考情报星球：

<https://planet.vulbox.com/detail/MTUxOTc=>

应急响应科技

附录 hw 漏洞情报清单（该清单漏洞未确认真实性，仅供参考）：

爆发日期	漏洞名称	利用条件	PoC 或 EXP
2023 年 8 月 9 日	某景 eHR SQL 注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某微 E-Office9 文件包含漏洞	需要用户登录	已有公开 PoC
2023 年 8 月 9 日	W*S Office for Windows 存在高危 0day 漏洞	需要用户交互	已有公开 PoC
2023 年 8 月 9 日	某信服应用交付报表系统远程命令执行漏洞	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某帆 OA SQL 注入漏洞 (1day)	远程未授权	暂无公开详细情报
2023 年 8 月 9 日	某软反序列化漏洞绕过漏洞	远程未授权	暂无公开详细情报
2023 年 8 月 9 日	某华智慧园区综合管理平台 SQL 注入漏洞	远程未授权	暂无公开详细情报
2023 年 8 月 9 日	某景 eHR OfficeServer.jsp 任意文件上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某达 OA SQL 注入漏洞 (CVE-2023-4165)	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某达 OA SQL 注入漏洞	远程未授权	已有公开 PoC

	(CVE-2023-4166)		
2023 年 8 月 9 日	某微 e-Office ajax.php 任意文件上传漏洞 (CVE-2023-2523)	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某微 e-Office9 文件上 传漏洞 (CVE-2023-2648)	远程未授权	已有公开 PoC
2023 年 8 月 9 日	*xchange Server 远程 代码执行漏洞 (CVE-2023-38182)	远程未授权	暂无公开详细 情报
2023 年 8 月 9 日	某远 OA wpsAssistServlet 任意 文件上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某捷 RG-BCR860 后台 命令注入 (CVE-2023-3450)	远程未授权	已有公开 PoC
2023 年 8 月 9 日	S**rtbi 在特定场景下 设置 Token 回调地址漏洞	远程未授权	暂无公开详细 情报
2023 年 8 月 9 日	某恒明御运维审计与风险 控制系统 service 任意 用户添加漏洞	远程未授权	暂无公开详细 情报
2023 年 8 月 9 日	某捷 EWEB 管理系统远	远程未授权	暂无公开详细

	程 代 码 注 入 漏 洞 (CVE-2023-34644)		情报
2023 年 8 月 9 日	某御安全网关 命令执行 漏 洞 (CNVD-2023-03898)	远程未授权	暂无公开详细 情报
2023 年 8 月 9 日	某联达 OA SQL 注入漏洞	需要登录后 台	已有公开 PoC
2023 年 8 月 9 日	某联达 OA 后台文件上 传漏洞	需要登录后 台	已有公开 PoC
2023 年 8 月 9 日	Hi**ISION 综合安防管 理平台 files 任意文件上 传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 9 日	Hi**ISION 综合安防管 理平台 report 任意文件 上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某神 SecGate 3600 防 火墙 obj_app_upfile 任 意文件上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某神 SecSSL 3600 安 全接入网关系统 任意密 码修改漏洞	远程未授权	已有公开 PoC
2023 年 8 月 9 日	某得 SRM tomcat.jsp	远程未授权	已有公开 PoC

	登录绕过漏洞		
2023 年 8 月 9 日	某信景云终端安全管理系统 login SQL 注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某友移动管理系统 uploadApk.do 任意文件上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某企互联 OA 文件读取漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某微 E-Cology ifNewsCheckOutByCurrentUser 某版本 SQL 注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某和 OA C6-GetSqlData.aspx SQL 注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某华智慧园区综合管理平台 searchJson SQL 注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某华智慧园区综合管理平台 文件上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某友时空 KSOA PayBill SQL 注入漏洞	远程未授权	已有公开 PoC



2023 年 8 月 10 日	某盟 SAS 堡垒机 local_user.php 任意用 户登录漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某盟 SAS 堡垒机 GetFile 任意文件读取漏 洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某盟 SAS 堡垒机 Exec 远程命令执行漏洞	远程未授权	已有公开 PoC
2023 年 8 月 10 日	某恒明御运维审计与风险 控制系统 xmlrpc.sock 任意用户添加漏洞	远程未授权	已有公开 PoC
2023 年 8 月 11 日	某明星辰-4A 统一安全管 控平台 getMater 信息泄 漏	远程未授权	已有公开 PoC
2023 年 8 月 13 日	某信服数据中心管理系统 XML 实体注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 13 日	某微 HrmCareerApplyPerVie w sql 注入漏洞	远程未授权	暂无公开详细 情报
2023 年 8 月 13 日	某约锁电子签章系统 远 程代码执行漏洞	远程未授权	已有公开 PoC
2023 年 8 月 13 日	某华智慧园区 任意密码	远程未授权	已有公开 PoC

	读取漏洞		
2023 年 8 月 13 日	某天动力 oa8000 SQL 注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 14 日	某赛通任意文件上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 14 日	某我行 CRM SQL 注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 14 日	某恒迷网远程命令执行漏洞	远程未授权	暂无公开详细情报
2023 年 8 月 14 日	某望制造 ERP 远程命令执行漏洞	远程未授权	已有公开 PoC
2023 年 8 月 14 日	*fficeWeb365 远程代码执行漏洞	远程未授权	已有公开 PoC
2023 年 8 月 15 日	J**cg-Boot 远程代码执行漏洞	远程未授权	已有公开 PoC
2023 年 8 月 15 日	某恒明御安全网关远程命令执行漏洞	远程未授权	已有公开 PoC
2023 年 8 月 15 日	某远 OA M1Server 反序列化	远程未授权	已有公开 PoC