# 2023 攻防演习每日情报汇总

漏洞盒子

2023-8-11

来到第三天，大家都在社区中讨论起了那些年 HVV 期间写的小说，HVV 期间遇到的奇葩事件，HVV 期间收到的花式钓鱼邮件以及 HVV 期间炫过的零食。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

- **某星辰-4A 统一安全管控平台信息泄漏：**漏洞等级中危，确认 nday 漏洞，POC 公开；7.0 为安全版本。披露时间：2023/8/11
- **某信源终端安全管理系统存在远程代码执行漏洞：**漏洞等级严重，确认 0day 漏洞，POC 小范围流传；影响试 6.8 及以下版本，漏洞披露时间：2023/8/11
- **某友时空 KSOA SQL 注入漏洞：**漏洞等级高危，确认 0day 漏洞，POC 公开；影响至最新版，漏洞披露时间：2023/8/11
- **某和 OA SQL 注入漏洞：**漏洞等级高危，确认为 0day 漏洞，POC 小范围流传；影响版本未知，漏洞披露时间：2023/8/11

- **某蝶 K3ERP 系统 SQL 注入：**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：2023/8/11
- **某华智慧园区综合管理平台 deleteFtp 接口远程命令执行漏洞：**漏洞等级严重，可能为 0day 漏洞，POC 未公开；影响版本未知，漏洞披露时间：2023/8/11
- **某元 EOS jmxjmx 反序列化漏洞：**漏洞等级严重，可能为 0day 漏洞，POC 未公开；影响版本未知，漏洞披露时间：2023/8/11
- **某元 EOS remote 反序列化漏洞：**漏洞等级严重，可能为 0day 漏洞，POC 未公开；影响版本未知，漏洞披露时间：2023/8/11
- **某鹰安全科技终端安全系统 SQL 注入漏洞：**漏洞等级高危，可能为 0day 漏洞，POC 未公开；影响版本：≤ 9.0 2022.10.18.12，漏洞披露时间：2023/8/11

## 1.2 红队投毒案例精选

- **利用红队工具进行投毒**

斗象情报中心侦测到红队工具投毒：https://github.com/TonyNPham/GodzillaPlugin-Suo5-MemProxy，样本 md5：fc0669c42c96fb9008faab07d5b8c4f3。

```
public class Suo5MemProxy extends ClassLoader implements Plugin {
    private final JButton runButton;
    private Payload H;
    private int[] g;
    private final JButton unLoadMemoryShellButton;
    private final JTextField M;
    private static final String[] m = {ALLATORIxDEMO("m;Q{m+L8R+J"), ALLATORIxDEMO("\u001dK!\u000b\bW\"J+L")};
    private final JLabel C;
    private int[] j;
    private Encoding k;
    private int[] b;
    private final JLabel F;
    private final JComboBox<String> f;
    private int[] d;
    private ShellEntity J;
    private byte[] i;
    private final JPanel ALLATORIxDEMO = new JPanel(new BorderLayout());
    private final String A = System.getProperty(ALLATORIxDEMO("Q=\u0010 _#[")).toLowerCase();
    private final String B = System.getProperty(ALLATORIxDEMO("Q=\u0010/L-V"));
    private final RTextArea a = new RTextArea();
    private final JSplitPane D = new JSplitPane();
```

代码使用 ALLATORI 混淆了解密后看代码发现 icon.png 里面有蹊跷，根据代码逻辑逆推出里面藏了一个 class 文件，然后 class 会释放出一个文件名开头为 microsoft10192 结尾为 cache 的文件（其实是个 dll 文件）。


当加载此插件后会外连到 45.76.176.189:443

## 2、 漏洞验证及复现

### 2.1 某和 OA C6-GetSqlData.aspx SQL 注入漏洞

由于系统未对用户输入进行过滤，未授权攻击者可以直接执行命令。

**漏洞复现截图:**

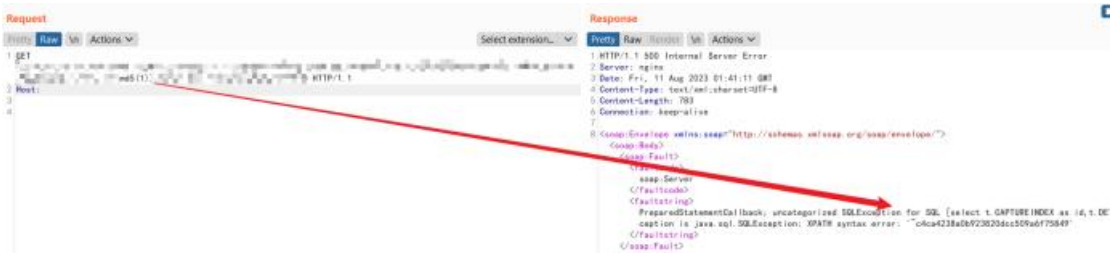

**修复建议:**

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。

### 2.2 某华智慧园区综合管理平台 searchJson SQL 注入漏洞

由于系统未对用户输入进行过滤，未授权攻击者可以直接执行命令。

**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 某华智慧园区综合管理平台 文件上传漏洞

系统未对用户输入内容进行过滤，导致攻击者可以上传恶意 Webshell 文件。

**漏洞复现截图:**

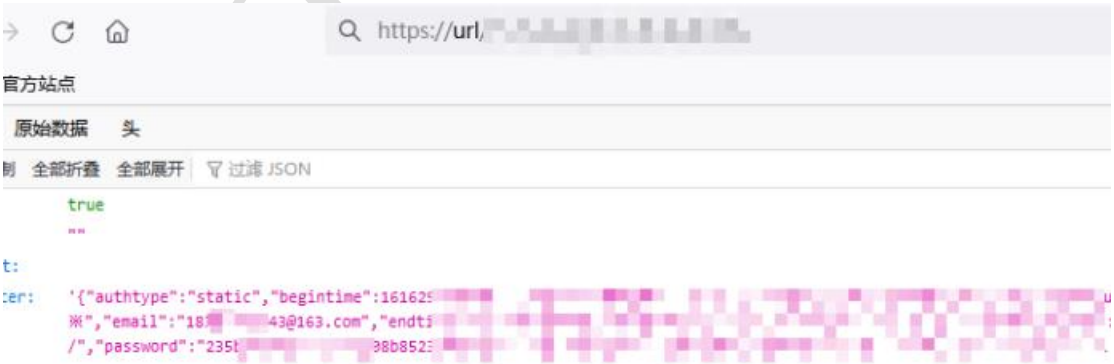

**修复建议：**

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。

## 2.4 某明星辰-4A 统一安全管控平台 getMater 信息泄漏

攻击者构造可以访问未授权的接口，从而获取敏感信息。

**漏洞复现截图:**




**修复建议：**

请使用此产品的用户尽快更新至最新版本。

## 2.5 某康综合安防 信息泄漏

攻击者构造可以访问未授权的接口，从而获取敏感信息。

**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。

## 2.6 某友时空 KSOA PayBill SQL 注入漏洞

由于系统未对用户输入进行过滤，未授权攻击者可以直接执行命令。

**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。

## 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. 某信源终端安全管理系统存在远程代码执行漏洞

   https://planet.vulbox.com/detail/MTQwMDI=

2. 关于安恒蜜罐逃逸的澄清说明

   https://planet.vulbox.com/detail/MTM5NDU=

3. 某网安中心共享疑似未公开漏洞情报

   https://planet.vulbox.com/detail/MTM5NzE=

4. 疑似钓鱼网站已有人中招

   https://planet.vulbox.com/detail/MTQwMDM=

5. 某友时空 KSOA PayBill SQL 注入漏洞

   https://planet.vulbox.com/detail/MTM5NTk=

   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/1689926987461824512

『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

## 4、 疑似红队攻击 IP 汇总

斗象情报中心在攻防第二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 |
| --- | --- | --- |
| 2023/8/11 | 192.241.201.85 | 美国加利福尼亚州旧金山 DigitalOcean 数据中心 |
| 2023/8/11 | 162.216.150.240 | 美国南卡罗来纳州蒙克斯科纳 Google 云 |
| 2023/8/11 | 221.5.212.10 | 中国重庆联通 |
| 2023/8/11 | 119.123.49.29 | 中国广东深圳市南山区电信 |
| 2023/8/11 | 35.203.210.183 | 美国 Merit 网络公司 |
| 2023/8/11 | 89.248.165.43 | 荷兰 |
| 2023/8/11 | 64.62.197.51 | 美国加利福尼亚州弗里蒙特市 Hurricane Electric 公司 |
| 2023/8/11 | 139.59.68.252 | 印度卡纳塔克邦班加罗尔 DigitalOcean 数据中心 |
| 2023/8/11 | 117.136.8.171 | 中国上海移动/GSM/TD-SCDMA/LTE 共用出口 |

| | | |
|---|---|---|
| 2023/8/11 | 192.241.195.83 | 美国加利福尼亚州旧金山 DigitalOcean 数据中心 |
| 2023/8/11 | 146.88.241.109 | 美国 |
| 2023/8/11 | 8.132.233.226 | 中国阿里云 |
| 2023/8/11 | 91.148.190.206 | 保加利亚 |
| 2023/8/11 | 47.96.228.27 | 中国浙江杭州市阿里云 |
| 2023/8/11 | 123.160.221.18 | 中国河南郑州市电信 |
| 2023/8/11 | 60.205.206.98 | 中国北京阿里云 BGP 服务器 |
| 2023/8/11 | 36.106.167.108 | 中国天津电信 |
| 2023/8/11 | 101.133.226.161 | 中国上海阿里云 |
| 2023/8/11 | 171.212.117.148 | 中国四川成都市电信 |
| 2023/8/11 | 47.94.151.38 | 中国北京阿里云 |

更多疑似红队攻击 IP 请参考情报星球：

https://planet.vulbox.com/detail/MTQwNDI=

附录 hw 漏洞情报清单（该清单漏洞还未全部确认真实性）：

| 爆发日期 | 漏洞名称 |
| --- | --- |
| 2023/8/9 | 某服应用交付系统命令执行 |
| 2023/8/9 | 协同办公文档（DzzOfffice）未授权访问 |
| 2023/8/9 | 某微 OA 前台代码执行漏洞 |
| 2023/8/9 | 某微 oa 进后台漏洞 |
| 2023/8/9 | Ucl*ud 的未授权获取任意用户 cookie |
| 2023/8/9 | 某书客户端 RCE 漏洞 |
| 2023/8/9 | 某微 Eoffice V10 前台 RCE |
| 2023/8/9 | 某客推商城任意文件上传 |
| 2023/8/9 | 某玥堡垒机 0day |
| 2023/8/9 | 某御运维审计与风险控制系统堡垒机任意用户注册 |
| 2023/8/9 | XX 协同管理系统存在 SQL 注入 |
| 2023/8/9 | 某微 emobile  注入漏洞 |
| 2023/8/9 | 海**视综合安防前台文件上传漏洞 |
| 2023/8/9 | 某凌 OA 前台代码执行漏洞 |
| 2023/8/9 | 某远 M3Server-xxxx 反序列化漏洞 |
| 2023/8/9 | 某远 A8 V8 SP1 SP2 文件上传漏洞 |
| 2023/8/9 | 某元 EOS 前台代码执行漏洞 |
| 2023/8/9 | 某微 E-cology 后台文件上传漏洞 |
| 2023/8/9 | 某微 E-Mobile 任意用户登录 |

| | |
|---|---|
| 2023/8/9 | 某微 E-Office10 信息泄露后台+后台文件上传漏洞 |
| 2023/8/9 | 某锁电子签章系统 RCE |
| 2023/8/9 | 某通电子文档平台文件上传漏洞 |
| 2023/8/9 | Idocview 命令执行漏洞 |
| 2023/8/9 | jeesite 代码执行漏洞 |
| 2023/8/9 | LiveBOS 文件上传漏洞 |
| 2023/8/9 | 某友 nc-cloud-任意文件写入 |
| 2023/8/9 | 某安信 VPN PWN |
| 2023/8/9 | xx IOA PWN |
| 2023/8/9 | xxx 准入 PWN |
| 2023/8/9 | eoffice9 前台文件包含 |
| 2023/8/9 | 某微 E-Cology ifNewsCheckOutByCurrentUser SQL 注入漏洞 |
| 2023/8/9 | fastjson 版本<2.0.27 存在高危反序列化漏洞 |
| 2023/8/9 | W*S 0day |
| 2023/8/9 | 某软 channel 序列化 |
| 2023/8/9 | 宏某 SQL 注入漏洞 |
| 2023/8/9 | 某微 E-Office9 文件包含漏洞 |
| 2023/8/9 | 某山 WPS 存在高危 0day 漏洞 |
| 2023/8/9 | 某服应用交付报表系统 远程命令执行漏洞 |
| 2023/8/9 | 某帆 OA SQL 注入漏洞(1day) |

| | |
|---|---|
| 2023/8/9 | 某软反序列化漏洞绕过漏洞 |
| 2023/8/9 | 某华智慧园区综合管理平台 SQL 注入漏洞 |
| 2023/8/9 | 宏某 eHR OfficeServer.jsp 任意文件上传漏洞 |
| 2023/8/9 | 某达 OA SQL 注入漏洞(CVE-2023-4165) |
| 2023/8/9 | 某达 OA SQL 注入漏洞(CVE-2023-4166) |
| 2023/8/9 | 某微 e-Office ajax.php 任意文件上传漏洞 (CVE-2023-2523) |
| 2023/8/9 | 某微 e-Office9 文件上传漏洞 (CVE-2023-2648) |
| 2023/8/9 | Exchange Server 远程代码执行漏洞 (CVE-2023-38182) |
| 2023/8/9 | 某远 OA wpsAssistServlet 任意文件上传漏洞 |
| 2023/8/9 | 某捷 RG-BCR860 后台命令注入 (CVE-2023-3450) |
| 2023/8/9 | 某迈特 在特定场景下设置 Token 回调地址漏洞 |
| 2023/8/9 | 某恒明御运维审计与风险控制系统 service 任意用户添加漏洞 |
| 2023/8/9 | 某捷 EWEB 管理系统远程代码注入漏洞 (CVE-2023-34644) |
| 2023/8/9 | 某恒明御安全网关 命令执行漏洞 (CNVD-2023-03898) |
| 2023/8/9 | 某联达 OA SQL 注入漏洞 |

| | |
|---|---|
| 2023/8/9 | 某联达 OA 后台文件上传漏洞 |
| 2023/8/9 | 某康综合安防管理平台 files 任意文件上传漏洞 |
| 2023/8/9 | 某康综合安防管理平台 report 任意文件上传漏洞 |
| 2023/8/9 | 某神 SecGate 3600 防火墙 obj_app_upfile 任意文件上传漏洞 |
| 2023/8/9 | 某神 SecSSL 3600 安全接入网关系统 任意密码修改漏洞 |
| 2023/8/9 | 某得 SRM tomcat.jsp 登录绕过漏洞 |
| 2023/8/9 | 某景云终端安全管理系统 login SQL 注入漏洞 |
| 2023/8/9 | 某友移动某系统 uploadApk.do 任意文件上传漏洞 |
| 2023/8/10 | 飞某联 OA 文件读取漏洞 |
| 2023/8/10 | 某联达 oa 后台文件上传漏洞 |
| 2023/8/10 | 某石网科 LMS 系统命令执行漏洞 |
| 2023/8/10 | 某翼云网页防篡改系统命令执行漏洞 |
| 2023/8/10 | 某麒麟堡垒机系统 SQL 注入漏洞 |
| 2023/8/10 | 某远 OA 系统命令执行漏洞 |
| 2023/8/10 | 某远 OA 系统 V5-V6 模块命令执行漏洞 |
| 2023/8/10 | 某石网科 EDR 系统 PHP 模块命令执行漏洞 |
| 2023/8/10 | 某华三 NX54 系统 web 模块信息泄露漏洞 |
| 2023/8/10 | 某捷 EG 易网关系统命令执行漏洞 |

| | |
|---|---|
| 2023/8/10 | 某华三 虚拟授权管理系统系统命令执行漏洞 |
| 2023/8/10 | 某华三 虚拟授权管理系统系统 web 模块命令执行漏洞 |
| 2023/8/10 | 某华三 综合日志审计平台系统命令执行漏洞 |
| 2023/8/10 | 某福迪 堡垒机系统 web 模块 SQL 注入漏洞 |
| 2023/8/10 | 某盟 SAS 堡垒机 localuser.php 任意用户登录漏洞 |
| 2023/8/10 | 某盟 SAS 堡垒机 GetFile 任意文件读取漏洞 |
| 2023/8/10 | 某盟 SAS 堡垒机 Exec 远程命令执行漏洞 |
| 2023/8/10 | 某康 综合安防管理平台 env 信息泄漏漏洞 |
| 2023/8/10 | 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 |
| 2023/8/10 | 某捷 NBR 路由器 fileupload.php 任意文件上传漏洞 |
| 2023/8/10 | 某华三 Magic CVE-2023-34928 远程代码执行漏洞 |
| 2023/8/10 | 某稀路由器命令执行漏洞 |
| 2023/8/10 | 某达 OA getdata 远程代码执行漏洞 |
| 2023/8/10 | 某帆 OA ioRepPicAdd 前台任意文件上传漏洞 |
| 2023/8/10 | 某思 OA wap.do SQL 注入漏洞 |
| 2023/8/10 | 某思 OA wap.do 任意文件下载漏洞 |
| 2023/8/11 | 安恒 明御运维审计与风险控制系统 xmlrpc.sock |

| | |
|---|---|
| | 任意用户添加漏洞 |
| 2023/8/11 | 启明星辰-4A 统一安全管控平台 getMater 信息泄漏 |
| 2023/8/11 | 泛微 E-Cology ifNewsCheckOutByCurrentUser 某版本 SQL 注入漏洞 |
| 2023/8/11 | 金和 OA C6-GetSqlData.aspx SQL 注入漏洞 |
| 2023/8/11 | 大华智慧园区综合管理平台 searchJson SQL 注入漏洞 |
| 2023/8/11 | 大华智慧园区综合管理平台 文件上传漏洞 |
| 2023/8/11 | 用友时空 KSOA PayBill SQL 注入漏洞 |
| 2023/8/11 | 某信源终端安全管理系统存在远程代码执行漏洞 |
| 2023/8/11 | 某蝶 K3ERP 系统 SQL 注入 |
| 2023/8/11 | 某华智慧园区综合管理平台 deleteFtp 接口远程命令执行漏洞 |
| 2023/8/11 | 某元 EOS jmxjmx 反序列化漏洞 |
| 2023/8/11 | 某元 EOS remote 反序列化漏洞 |
| 2023/8/11 | 某鹰安全科技终端安全系统 SQL 注入漏洞 |