2023 攻防演习每日情报汇总

漏洞盒子

2023-8-16

演练第八天，蓝对出局的小道消息满天飞，但多数消息不属实，估计是蓝队放出的烟雾弹，当然红队并没有被这些烟雾弹所迷惑，激烈的“厮杀”还在继续；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

- **某源云 ERP 文件上传漏洞：**漏洞等级严重，0day 漏洞，POC 小范围传播；影响至最新版本。披露时间：2023/8/16
- **某开普前置服务管理平台远程代码执行漏洞：**漏洞等级严重，0day 漏洞，POC 小范围传播；影响版本未知，漏洞披露时间：2023/8/16
- **某华车载系统文件上传漏洞：**漏洞等级严重，0day 漏洞，POC 小范围传播；影响版本未知，漏洞披露时间：2023/8/16
- **某信服 SG 上网优化管理系统任意文件读取漏洞：**漏洞等级高危，可能为 0day 漏洞，POC 公开；影响版本未知，漏洞披露时间：2023/8/16

- **某微 E-Mobile 敏感信息泄露：**漏洞等级高危，可能为 0day 漏洞，POC 小范围传播；影响版本未知，漏洞披露时间：2023/8/16
- **某方通远程代码执行漏洞：**漏洞等级严重，为 1day 漏洞，POC 小范围传播；影响版本为不大于 7.0.4.9，存在补丁，漏洞披露时间：2023/8/16
- **某捷通 T+反序列化漏洞：**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：2023/8/16
- **某空智友企业流程化管控系统 SQL 注入漏洞：**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：2023/8/16

1.2 红队投毒案例精选

- **利用邮件进行钓鱼**

斗象情报中心侦测到红队投毒，样本 SHA256： 3a89096753e33eacbc93a3f2f0abaa962fc941bd893d31cd65a92e4184de4326。

外连 IP：101.42.14.53

邮件主题：关于 xx 集团被钓鱼邮件攻击事件的预警通知

邮件发件人：人力资源部

相关样本：**123.exe**(f57e718d496252b09f33c47d2dfcb30559f84bea4ee2019a33242f3d76fb36f5)

情报来源：https://planet.vulbox.com/detail/MTUzNTU=

- **利用邮件进行钓鱼**

斗象情报中心侦测到红队投毒，样本 SHA256： cc283c106fbd931750e08dcb6a19b2f82204b6372dd2c4e831e37784194a0a9b。

外连 IP：139.224.17.133

邮件主题：关于公司 OA 系统更新的通知

相关样本：**6hyF**(b990edcee73aa14f8a104edc5c68afe06c8732fd7a5bdfebbed551fa9144b5c4)

情报来源：https://planet.vulbox.com/detail/MTUyOTM=

- **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。

外连域名：ksu-1312459886.cos.ap-guangzhou.myqcloud.com(36.248.13.172)

邮件主题：供应商报名信息表、公司资质材料证明文件等汇总材料

相关样本：**【2023 年】海南航空_商务洽谈函_2023 年 8 月 14 日.exe**(596c

96a30a3fe7ac35b6dc2d691a7ba16e32a364dad1a78a0b07737e1cd0c211)、**关于方大航空食品（北京）有限公司配餐楼消防维修采购项目违规操作投诉.rar**(0e442cfaa0c16a434d976baf6da36310dd5532d8df9030bd13abd6fea2290c2e)、**【2023 年】祥瑞航空_商务洽谈函_2023 年 8 月.exe**(dfe669269b6353642ba58e50c7adc6f101656608a0d2117d9b2425bfe56612be)、**个人简历-赵莉莉-首都经济贸易大学.exe**(6bc9b635c5878da5849d4da9ec6d247784b9cb7ea5228cd167c8adba661243eb)、**个人简历_郑先生_上海对外贸易大学_计算机科学与技术_202308　　[副本].exe**(f5158c075f6d615b9b23078e32b10bd3a1106035bb6b78c506fa3cd73c915c2f)、**关于方大航空食品（北京）有限公司配餐楼消防维修采购项目违规操作投诉.exe**(7751e46042e9e8ff97198c3db184f65392fc55e7eb1b53a2a7b0ba3eb8cc4dc6)、**北京洁简天兴商贸有限责任公司报名航空股份机上经济舱洗漱包项目资质文件.exe** (a970e59b6f346ac603500649065511b98866f2a4ab5eb94975dfe371e624deca)**等**

情报来源：https://planet.vulbox.com/detail/MTUyOTc=

2、 漏洞验证及复现

2.1 某源云 ERP 文件上传漏洞

未授权的攻击者构造特制的压缩包进行上传，系统解压时会造成 zip-silp 导致恶意文件被上传至 Web 目录下，从而被攻击者进行利用。

漏洞复现截图:

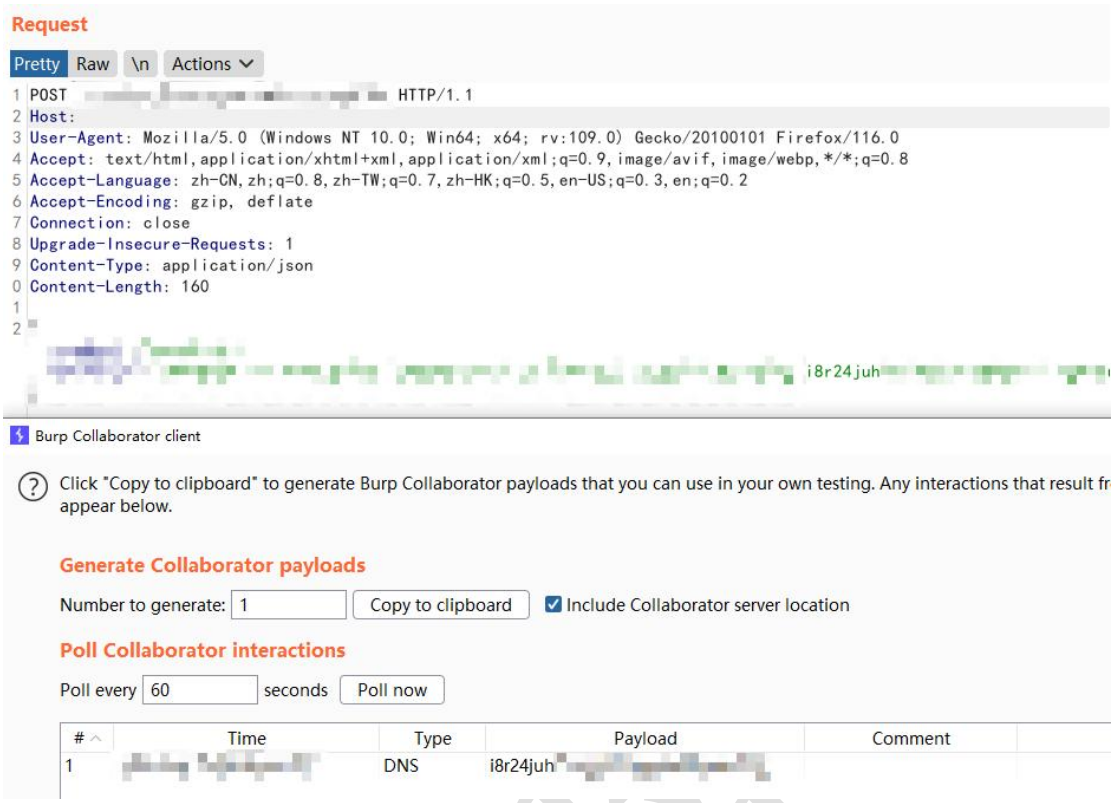
修复建议:

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 某开普前置服务管理平台 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 某华车载系统文件上传漏洞

未授权攻击者可以构造特制的请求上传 Webshell 文件，进而控制服务器。

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. 【讨论】Chrome v8 Sandbox 绕过

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

2. 某方通更新安全补丁

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

3. 某微 E-Mobile 敏感信息泄露

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

4. 某华车载系统 任意文件上传

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

   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/1691770416047198208

5. 某御 SQL 注入

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

『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八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
8/16/2023	120.78.154.28	中国广东深圳市阿里云
8/16/2023	106.58.222.2	中国云南电信/数据上网公共出口
8/16/2023	8.134.206.129	中国广东深圳市阿里云
8/16/2023	180.76.162.44	中国北京北京百度网讯科技有限公司 BGP 节点
8/16/2023	39.105.194.126	中国北京阿里云
8/16/2023	47.107.53.20	中国广东深圳市阿里云
8/16/2023	182.42.30.83	中国内蒙古电信/呼和浩特市电信天翼云计算数据中心
8/16/2023	43.139.87.118	中国广东广州市腾讯云
8/16/2023	222.213.236.234	中国四川雅安市电信
8/16/2023	39.108.11.115	中国广东深圳市阿里云
8/16/2023	8.129.57.116	中国阿里云
8/16/2023	101.43.205.36	中国北京腾讯云
8/16/2023	81.68.159.12	中国上海腾讯云
8/16/2023	1.117.176.229	中国上海腾讯云
8/16/2023	96.8.117.232	美国纽约州伊利县威廉斯维尔村 ColoCrossing 有限公司
8/16/2023	39.105.143.25	中国北京阿里云

	0	
8/16/2023	1.117.204.147	中国上海腾讯云
8/16/2023	182.92.71.216	中国北京阿里云
8/16/2023	82.157.238.74	中国北京腾讯云
8/16/2023	47.97.74.126	中国浙江杭州市阿里云

更多疑似红队攻击 IP 请参考情报星球：

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

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 HrmCareerApplyPerView 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
2023 年 8 月 16 日	某源云 ERP 文件上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 16 日	某开普前置服务管理平台远程代码执行漏洞	远程未授权	已有公开 PoC

2023 年 8 月 16 日	某华车载系统文件上传漏洞	远程未授权	已有公开 PoC
2023 年 8 月 16 日	某信服 SG 上网优化管理系统任意文件读取漏洞	远程未授权	已有公开 PoC
2023 年 8 月 16 日	某微 E-Mobile 敏感信息泄露	远程未授权	暂无公开详细情报
2023 年 8 月 16 日	某方通远程代码执行漏洞	远程未授权	暂无公开详细情报
2023 年 8 月 16 日	某空智友企业流程化管控系统 SQL 注入漏洞	远程未授权	已有公开 PoC
2023 年 8 月 16 日	某捷通 T+反序列化漏洞	远程未授权	已有公开 PoC