2023 攻防演习每日情报汇总

漏洞盒子

2023-8-13

第五天，红队的小伙伴们开始发力，各种告警也多了起来，同时流传红队拿下一些行业靶标可获取 6 倍积分，蓝队的小伙伴们又有的忙了；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

- **某和 OA SQL 注入漏洞：**漏洞等级高危，0day 漏洞，POC 公开；影响版本未知。披露时间：2023/8/13
- **某时空 KSOA SQL 注入漏洞：**漏洞等级严重，确认 0day 漏洞，POC 公开；影响版本未知，漏洞披露时间：2023/8/13
- **某信服数据中心管理系统外部实体注入漏洞：**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：2023/8/13
- **某华智慧园区任意密码读取漏洞：**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：2023/8/13

- **某约锁电子签章系统远程代码执行漏洞：**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：2023/8/13
- **某微 SQL 注入漏洞：**漏洞等级高危，可能为 0day 漏洞，POC 未公开；影响版本未知，漏洞披露时间：2023/8/13
- **某天动力 oa8000 SQL 注入漏洞：**漏洞等级高危，可能为 0day 漏洞，POC 未公开；影响版本未知，漏洞披露时间：2023/8/13

1.2 红队投毒案例精选

- **利用 hvv 漏洞合集进行投毒**

斗象情报中心侦测到红队投毒，样本 SHA256： 58b73f87b28664b71f23133ea270ee1c28e6f4002e134bac214fa277618cecff。

外连可疑 IP：149.28.157.158

相关样本还有：**654a9d346319642b_nothing.exe**(654a9d346319642bfdcde85e7e5ddd64096f7b8fcd6c1a3c301aafdf9c9a8006)、**2023Hvv 0day 收集.zip**(0d06663d70b2c808d67d78090dc2b51446935c1fa1b3f69f85fe3cd94603935f)

2、 漏洞验证及复现

2.1 某华智慧园区综合管理平台任意用户密码读取漏洞

由于系统未对接口进行身份认证，导致攻击者在指定 userName 参数后可以获取用户的密码。

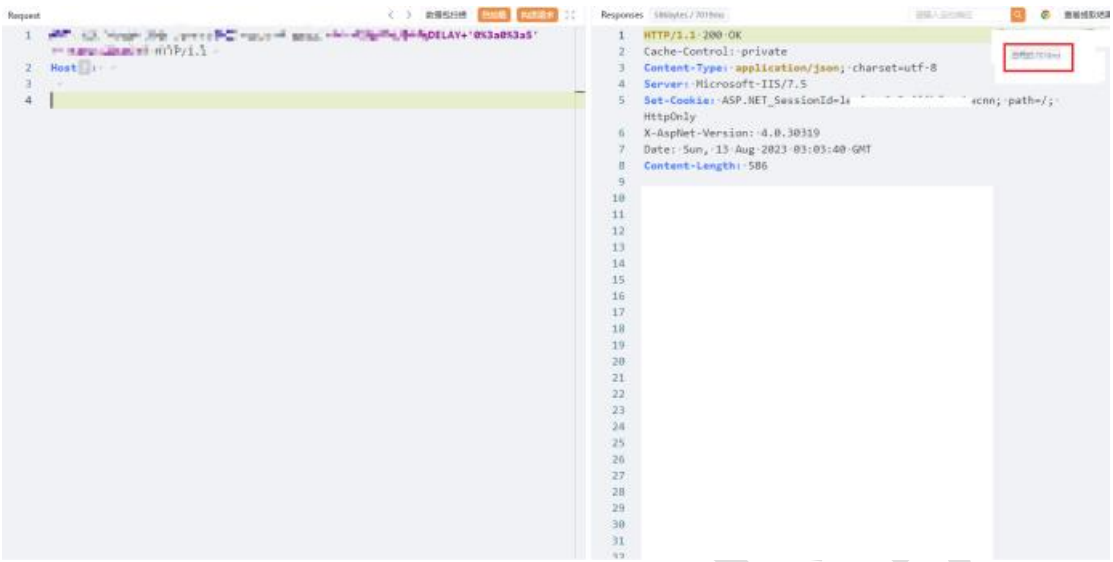
漏洞复现截图:

修复建议：请使用该产品的用户尽快对 /admin/user_getUserInfoByUserName.action 路由进行过滤，防止外部 IP 进行访问。

2.2 某和 OA GetTreeDate SQL 注入漏洞

由于系统未对用户输入进行过滤，导致未授权攻击者可以通过 id 参数进行 SQL 注入，获取敏感信息。

漏洞复现截图:



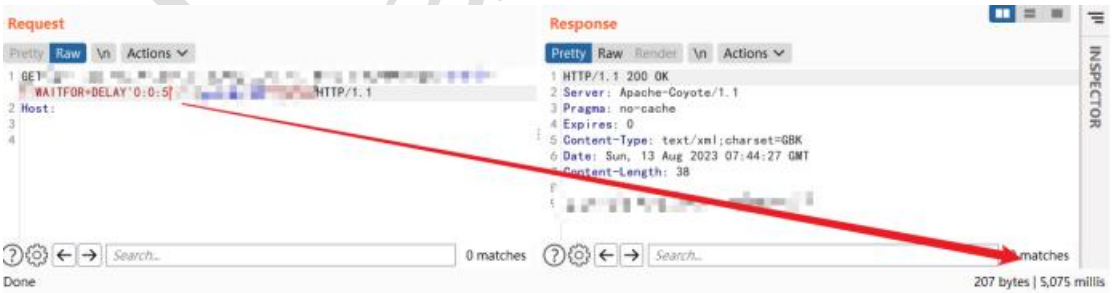
修复建议：

请使用该产品的用户尽快 WAF 设备对其进行过滤。

2.3 某友时空 KSOA TaskRequestServlet SQL 注入漏洞

由于系统未对用户输入进行过滤，导致未授权攻击者可以通过 unitid 参数进行延时注入，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。

2.4 某友时空 KSOA imagefield SQL 注入漏洞

由于系统未对用户输入进行过滤，导致未授权攻击者可以通过 sKeyvalue 参数进行联合查询，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。

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. 疑似技战法存在钓鱼

   https://planet.vulbox.com/detail/MTQ2MzA=

2. 某华车载监控平台存在任意文件上传漏洞

   https://planet.vulbox.com/detail/MTQ1ODE=

3. 某凌 EKP 远程代码执行漏洞

   https://planet.vulbox.com/detail/MTQ1OTk=

4. 恶意 C2 地址

   https://planet.vulbox.com/detail/MTQ2NjY=

5. 某友时空 KSOA TaskRequestServlet SQL 注入漏洞

   https://planet.vulbox.com/detail/MTQ2MjU=

   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/1690667006510108672

『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五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
2023/8/13	140.75.182.80	中国山东青岛市电信
2023/8/13	125.121.21.162	中国浙江杭州市电信
2023/8/13	114.116.120.25	中国北京华为云
2023/8/13	222.131.62.161	中国北京联通
2023/8/13	59.172.4.198	中国湖北武汉市电信
2023/8/13	27.151.84.31	中国福建福州市电信
2023/8/13	175.102.180.48	中国上海上海有孚计算机网络有限公司
2023/8/13	180.158.10.167	中国上海电信
2023/8/13	118.24.215.121	中国重庆腾讯云
2023/8/13	223.167.150.198	中国上海联通
2023/8/13	123.182.168.143	中国河北廊坊市电信
2023/8/13	221.239.221.231	中国上海嘉定区电信
2023/8/13	180.109.219.188	中国江苏南京市电信
2023/8/13	61.160.213.169	中国江苏常州市电信

更多疑似红队攻击 IP 请参考情报星球：

https://planet.vulbox.com/detail/MTQ2ODU=

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
2023/8/12	企业某信信息泄露
2023/8/12	某信天擎终端安全管理系统信息泄露
2023/8/12	某望制造 ERP 远程命令执行漏洞
2023/8/12	某我行 CRM SQL 注入漏洞

2023/8/12	某云 APPHUB 未授权访问
2023/8/12	某友 M1 反序列化命令执行漏洞
2023/8/12	广某达 LinkworksSQL 注入漏洞
2023/8/12	某友 U8 CRM 客户关系管理系统任意文件读取漏洞
2023/8/12	MilesightVPN 任意文件读取漏洞
2023/8/12	某盘微信管理平台未授权访问漏洞
2023/8/12	某御 ACM 上网行为管理系统 SQL 注入漏洞
2023/8/12	某信服数据中心管理系统 XML 实体注入漏洞
2023/8/12	某微 HrmCareerApplyPerView sql 注入漏洞
2023/8/12	某约锁电子签章系统 远程代码执行漏洞
2023/8/12	某华智慧园区 任意密码读取漏洞
2023/8/12	某天动力 oa8000 SQL 注入漏洞