2023 攻防演习每日情报汇总

漏洞盒子

2023-8-12

来到第四天，周六也没有让红蓝队有丝毫的懈怠，高危 0day 漏洞层出不穷，也让本次攻防演练的对抗愈加激烈；言归正传，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

- **企业某信存在信息泄露：**漏洞等级严重，0day 漏洞，POC 公开；影响企业微信私有化（含政务微信）、2.5.x 版本、2.6.930000 以下版本。披露时间：2023/8/12
- **某信天擎终端安全管理系统信息泄露：**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：2023/8/12
- **某望制造 ERP 远程命令执行漏洞：**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：2023/8/12
- **某我行 CRM SQL 注入漏洞：**漏洞等级高危，确认为 0day 漏洞，POC 公

开；影响版本未知，漏洞披露时间：2023/8/12

- **某云 APPHUB 未授权访问：**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：2023/8/12
- **某友 M1 反序列化命令执行漏洞：**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：2023/8/12

1.2 红队投毒案例精选

- **利用简历进行投毒**

斗象情报中心侦测到红队简历投毒，样本 SHA256： fbe3e418e794cca842e39fbf7de902970dcdb954d53491d71fcec6f60a87acd0。

外连三个可疑 IP：47.94.158.102、39.105.153.187、8.134.148.252

相关样本还有：招标文件.rar(3bb249ea0e744cc6365da6d612d1feb7cac89bc6fc3e77390e136b7159843a49)、[招标文件]贵州龙溪招标投递相关文件20230809S604.exe(e3db1828c831a7baebf94f5e125aaf36e4e664c03fdb64e26f0ff3970721720d)

各位蓝队请关注并采取相应的防御策略。

2、 漏洞验证及复现

2.1 企业某信信息泄露

由于系统未对接口进行身份认证，未经身份验证的攻击者可以获取 corpid 和 Secret，进而获取 access_token。

漏洞复现截图:

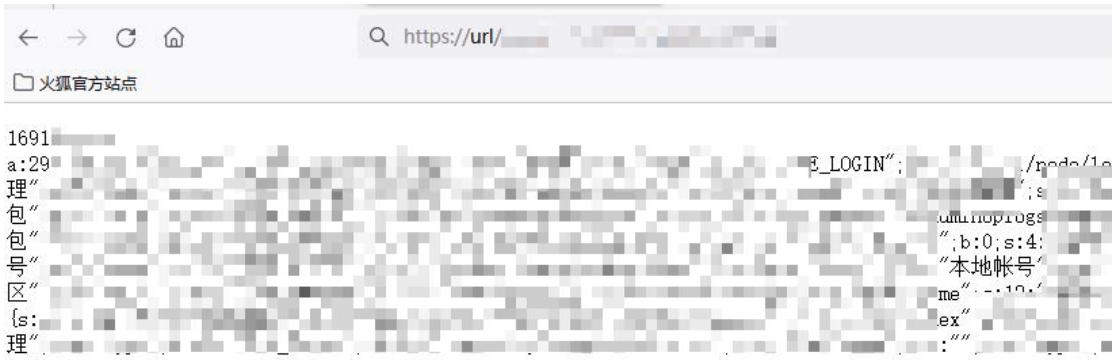
影响版本：企业微信私有化（含政务微信）、2.5.x 版本、2.6.930000 以下版本

修复建议：请使用该产品的用户尽快对 /cgi-bin/gateway/agentinfo 路由进行过滤

2.2 某安信天擎终端安全管理系统信息泄露

由于系统未对接口进行身份认证，未授权攻击者可以通过该接口获取敏感信息。

漏洞复现截图:



修复建议:

请使用该产品的用户尽快对 /runtime/admin_log_conf.cache 路由进行过滤。

2.3 某御 ACM 上网行为管理系统 SQL 注入漏洞

由于系统未对用户输入进行过滤，未授权攻击者可以利用该漏洞获取数据库中敏感数据。

漏洞复现截图:

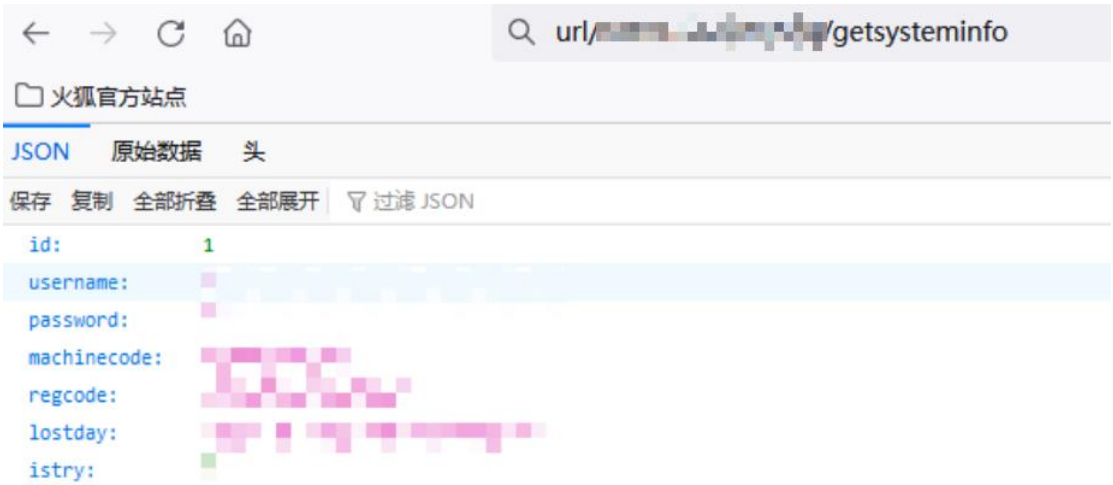
修复建议:

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 某盘微信管理平台未授权访问漏洞

系统未对接口进行身份认证，未授权攻击者可以通过该接口获取敏感信息。

漏洞复现截图:



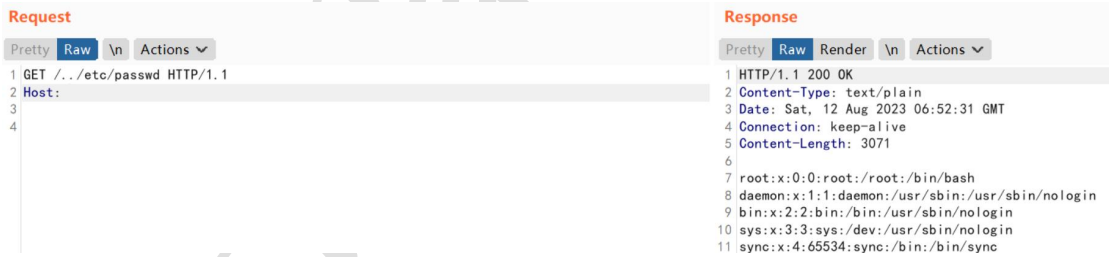
修复建议：

请使用该产品的用户尽快对 /admin/weichatcfg/getsysteminfo 路由进行过滤。

2.5 MilesightVPN 任意文件读取漏洞

攻击者构造可以利用"../"读取服务器中的文件内容。

漏洞复现截图:



修复建议：

请使用此产品的用户对 "../" 进行过滤处理。

2.6 某友 U8 CRM 客户关系管理系统任意文件读取漏洞

攻击者可以访问未授权的接口，从而读取服务器中的任意文件。

漏洞复现截图:

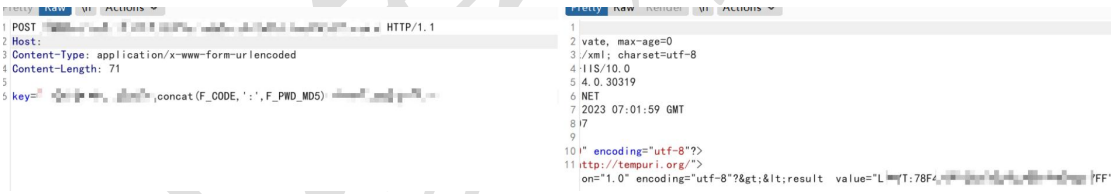
修复建议：

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。

2.7 广某达 LinkworksSQL 注入漏洞

由于系统未对用户输入进行过滤，未授权攻击者可以利用该漏洞读取。

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. 某望制造 ERP comboxstore.action 远程命令执行漏洞

   https://planet.vulbox.com/detail/MTQ0MTA=

2. 0day！企业某信可被获取全量数据

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

   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/1690302744709173248

3. 某云 APPHUB 未授权访问预警

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

4. 疑似未公开的多个漏洞预警

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

5. 某信天擎终端安全管理系统信息泄露

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

   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/1690304248983719936

『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四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
2023/8/12	52.193.254.137	美国华盛顿州西雅图市亚马逊(Amazon)公司数据中心
2023/8/12	52.167.144.71	美国弗吉尼亚州梅克伦堡县博伊顿 Microsoft
2023/8/12	52.167.144.98	美国弗吉尼亚州梅克伦堡县博伊顿 Microsoft
2023/8/12	5.255.121.111	荷兰
2023/8/12	49.71.154.34	中国江苏泰州市电信
2023/8/12	89.248.163.87	荷兰
2023/8/12	98.142.141.184	美国加利福尼亚州洛杉矶 IT7 网络
2023/8/12	87.121.221.63	保加利亚
2023/8/12	82.157.64.129	中国北京腾讯云
2023/8/12	119.8.126.102	中国香港华为云
2023/8/12	119.82.135.226	越南
2023/8/12	119.61.0.140	中国北京电信/二六三网络

		通信电信数据中心
2023/8/12	119.237.153.195	中国香港电讯盈科有限公司
2023/8/12	119.91.204.187	中国广东广州市腾讯云
2023/8/12	119.28.49.135	中国香港腾讯云
2023/8/12	119.3.175.5	中国北京华为云
2023/8/12	119.91.192.7	中国广东广州市腾讯云
2023/8/12	119.29.7.161	中国广东广州市腾讯云
2023/8/12	119.254.89.3	中国北京光环新网电信数据中心
2023/8/12	119.18.149.54	孟加拉

更多疑似红队攻击 IP 请参考情报星球：

https://planet.vulbox.com/detail/MTQ0MTg=

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

8/12/2023	某云 APPHUB 未授权访问
8/12/2023	某友 M1 反序列化命令执行漏洞
8/12/2023	广某达 LinkworksSQL 注入漏洞
8/12/2023	某友 U8 CRM 客户关系管理系统任意文件读取漏洞
8/12/2023	MilesightVPN 任意文件读取漏洞
8/12/2023	某盘微信管理平台未授权访问漏洞
8/12/2023	某御 ACM 上网行为管理系统 SQL 注入漏洞