微步在线

2023

0809

快报内容总结

EXPRESS NEWS CONTENT SUMMARY

一、IP 快报

IP 信息	特征行为
203.15.0.220	扫描
8.130.23.133	扫描
36.134.6.166	扫描
101.132.223.4	扫描
113.141.89.103	扫描
47.92.199.215	扫描
101.200.127.65	恶意云主机
106.55.107.106	恶意云主机
39.107.123.197	多种漏洞利用
61.181.206.56	多种漏洞利用
36.27.6.213	扫描
113.246.224.193	多种漏洞利用
182.92.69.156	多种漏洞利用
123.57.69.175	多种漏洞利用

二、漏洞快报

1、某 OA 前台存在 SQL 注入漏洞

漏洞来源：X 漏洞奖励计划

处置建议：使用网络 ACL 限制访问来源，加强监测。微步威胁感知平台 TDP 已支持检测，TDP 模型版本需要更新到 20230808XXXXXX 及以上版本；更新过版本的用户，TDP 已具备该检测能力；规则 ID：S3100119400、S3100119401、S3100119402、S3100119403

微步安全情报网关 OneSIG 2.4.1 已支持检测，规则更新包需要为：20230725

2、某终端安全系统存在 SQL 注入漏洞

漏洞来源：X 漏洞奖励计划

处置建议：使用网络 ACL 限制访问来源，加强监测。微步威胁感知平台 TDP 已支持检测，TDP 模型版本需要更新到 20230808XXXXXX 及以上版本；更新过版本的用户，TDP 已具备该检测能力；规则 ID：S3100119325、S3100119330；微步安全情报网关 OneSIG 2.4.1 已支持检测，规则更新包需要为：20230725

3、海*威视 iSecure Center 综合安防管理平台文件上传漏洞（XVE-2022-23348)

漏洞来源：X 漏洞奖励计划

处置建议：使用网络 ACL 限制访问来源，加强监测。

微步威胁感知平台 TDP 已支持检测，TDP 模型版本需要更新到 20230808XXXXXX 及以上版本；更新过版本的用户，TDP 已具备该检测能力；规则 ID：S3100031152、S3100031153；微步安全情报网关 OneSIG 2.4.1 已支持检测及拦截，规则包版本需要为：20230725

4、*捷 RIIL-BMC 综合业务管理系统命令执行漏洞（XVE-2022-28361)

漏洞来源：X 漏洞奖励计划

处置建议：使用网络 ACL 限制访问来源，加强监测。

微步威胁感知平台 TDP 已支持检测，TDP 模型版本需要更新到 20230808XXXXXX 及以上版本；更新过版本的用户，TDP 已具备该检测能力；规则 ID：S3100028516、

S3100028518；微步安全情报网关 OneSIG 2.4.1 已支持检测及拦截，规则包版本需要为：20230725

三、样本快报

1、文件名：["*擎 V10 紧急修复工具和相关问题方案上报详情-20230807.exe"]

SHA256：

34d8969a381957b70bb7873f115407fbd1db892a0793548aecd4e6f8649e6941

2、文件名：简历.exe

SHA256：

10a1b8c85242444c3009d81d6db5a6dc82e34739b225cc16ae134c8f89dd9e68

3、文件名：简历.exe

SHA256：

0e8fa671ccf765236665e8c61ef4e7d3b0be37482f466fce9def4f72703806af

4、文件名：关于官网注册后信息有关问题的反馈.exe

SHA256：

7f7990d7caebf089b056555f2e6c6519d58c38e0aa8276322c11175bfa3c987e