

奇安信网神安全分析与管理系统 SOAR

产品补丁升级公告

尊敬的奇安信客户：

近日，奇安信 CERT 监测到开源组件 Apache Log4j2 存在任意代码执行漏洞（CVE-2021-44228），我们第一时间奇安信网神安全分析与管理系统 SOAR（以下简称“SOAR”）进行了漏洞影响分析，于 2021 年 12 月 10 日提供漏洞影响和缓解加固措施说明，并于 2021 年 12 月 16 日发布了补丁包用于更新修复了漏洞的 Log4j2 组件版本。

SOAR 产品受影响版本：V4.0_6.5.0 至 V4.0_6.6.0

以下为补丁的详细说明：

1. 更新说明

该版本支持通过 SOAR admin 账号登录【系统->系统升级】模块上传升级包方式进行升级。

2. 已解决的问题

将 Apache log4j2 版本由 2.13.3 升级到 2.15.0-RC2 修复 Apache log4j 漏洞。

3. 其他说明

升级过程中会重启系统服务，造成产品功能业务短时中断，请知悉。由于软件安装的操作系统个别版本不同，未按安装手册要求安装（CentOS_7.X_x64 或 Redhat_7.X_x64 要求为“基础设施服务器安装”）的版本，可能有些老的版本会出现 dd 命令版本过高，SOAR 脚本升级命令未完全兼容的现象，导致升级失败。出现这种问题不会影响用户业务，请联系我公司二线人员解决。

4. 如何升级

您可以通过联系我公司销售、客户服务经理获取加固方案和升级方式，您也可以拨打 4009303120 进行咨询，我们将竭诚为您服务。

奇安信科技集团
2021 年 12 月 16 日