奇安信云安全管理平台补丁升级公告

尊敬的奇安信客户：

感谢您一直以来对奇安信公司的信赖与支持，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）。我们第一时间对奇安信云安全管理平台（CSMP）以及平台内安全组件进行了漏洞影响分析，并于 2021 年 12 月 10 日提供漏洞影响和缓解加固措施说明，同时发布补丁来修复平台以及安全组件 Apache Log4j2 远程代码执行漏洞。

以下为补丁的详细说明：

1. 更新说明

- 漏洞描述

Apache Log4j 被发现存在一处任意代码执行漏洞，由于 Apache Log4j2 某些功能存在递归解析功能，攻击者可直接构造恶意请求，触发远程代码执行漏洞。

- 影响范围：

  CSMP 版本<=2.0.5SP1

  堡垒机组件版本<=3.4.14.0

  LAS 日志审计组件版本<=V5.0_7.3.0

  HLAS 虚拟化日志审计组件版本<=3.6.6.316

  VNTA 云网安全分析组件所有发布版本

- 修复方式：

  1，CSMP 平台按照 csmp-log4j-hotfix-v1.0 升级包内操作说明，在集群里每台节点执行升级 bin 文件即可。

  2，堡垒机组件需要将堡垒机版本升级到 3.4.14.0 版本，然后页面上升级补丁包即可。

  3，LAS 日志审计建议先将 LAS V5.0_7.1.X\7.2.X 逐个升级至 V5.0_7.3.0 版本，再基于此版本安装补丁包即可。

  4，HLAS 虚拟化日志分析 3.6.6.314 以前版本下载修复脚本手动执行修复，3.6.6.316 版本下载升级包页面进行升级。

5，VNTA 运维安全分析后台执行 bin 升级文件即可。

2. 已解决的问题

Apache Log4j-2.x 版本漏洞修复。

3. 其他说明

强烈建议升级此版本。升级过程中会重启系统服务，请知悉。

4. 如何升级

您可以通过我公司官网下载相应升级版本，或联系我公司销售、客户服务经理获取升级方式，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