网络威胁态势感知系统 V2.0 版本升级公告

尊敬的奇安信客户，您好：

感谢您一直以来对奇安信公司的信赖与支持，为进一步提升产品的用户体验和可靠性，更好服务客户，我公司正式发布网络威胁态势感知系统 V2.0 产品的 V2.0(2.0.4.1、2.0.5.1、2.0.5.2)版本的漏洞修复补丁版本。此次发布的版本主要是修复开源组 Apache Log4j 任意代码执行漏洞（CVE-2021-44228），建议优先选择更新该版本。

以下为关于版本升级的详细说明：

1. 更新说明

漏洞描述

近日，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。态势感知产品采用了 Apache Log4j 记录日志，受该漏洞影响。

修复方式

该版本更新了开源组 Log4j 为最新 2.15.0-RC2 版本，该版本修复了 Apache Log4j 任意代码执行漏洞（CVE-2021-44228）。

该版本需通过人工上传升级包进行手工升级。

2. 已解决的问题

该版本修复了 Apache Log4j 任意代码执行漏洞（CVE-2021-44228）。

3. 其他说明

鉴于 Log4j 漏洞影响面较大，漏洞利用难度低，强烈建议完成此次升级。

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。

奇安信科技集团股份有限公司

2021 年 12 月 13 日