iMC&U-Center&AOM等业软产品是否涉及Apache Spark UI 命令注入漏洞

iMC EPS iMC WSM PLAT U-Center 2.0 贾海韵 2022-07-20 发表

漏洞相关信息

漏洞编号： CVE-2022-33891

漏洞名称： Apache Spark UI 命令注入漏洞

产品型号及版本： iMC&U-Center&AOM

漏洞描述

关于Apache Spark UI 命令注入漏洞的通告：

经集团总指挥部办公室分析研判，Apache Spark存在高危漏洞，Apache Spark 是美国阿帕奇（Apache）软件基金会的一款支持非循环数据流和内存计算的大规模数据处理引擎，如果Apache Spark UI 启用了 ACL，则HttpSecurityFilter 中的代码路径允许通过提供任意用户名来模拟执行。恶意用户能够访问权限检查功能，根据他们的输入构建一个 Unix shell 命令并执行。攻击者可利用此漏洞任意执行 shell 命令。鉴于该漏洞危害较大且 POC 已公开，建议用户尽快自查修复。

一、漏洞具体信息：

【漏洞编号】CVE-2022-33891

【影响范围】

org.apache.spark:spark-core_2.12@(∞, 3.1.3)

org.apache.spark:spark-core_2.12@[3.2.0, 3.2.2)

org.apache.spark:spark-core_2.13@[3.2.0, 3.2.2)

【漏洞描述】攻击者可利用此漏洞任意执行 shell 命令。

【规避措施】获取 spark 版本，判断其版本是否在 (∞, 3.1.3)、[3.2.0, 3.2.2)、[3.2.0, 3.2.2)范围中，升级 Apache Spark 到 3.1.3、3.2.2 或 3.3.0 或更高版本。

漏洞解决方案

以下产品皆不涉及该漏洞，可参考漏洞报告进行漏洞修复，不影响功能使用：
iMC PLAT，统一数字底盘，U-Center 1.0&2.0， AOM所有产品， EIA/EAD V7&V9，WSM V7&V9，EPS V7&V9。