iMC&U-Center1.0不涉及漏洞CVE-2022-24112

PLAT 陈冰洁 2022-03-23 发表

漏洞相关信息

漏洞编号： CVE-2022-24112

漏洞名称： Apache APISIX 存在改写 X-REAL-IP header 的风险公告

产品型号及版本： iMC_1.0系列产品，U-Center1.0系列产品

漏洞描述

在 Apache APISIX 2.12.1 之前的版本中（不包含 2.12.1 和 2.10.4），启用 Apache APISIX batch-requests 插件之后，会存在改写 X-REAL-IP header 风险。

该风险会导致以下两个问题：

- 攻击者通过 batch-requests 插件绕过 Apache APISIX 数据面的 IP 限制。如绕过 IP 黑白名单限制。
- 如果用户使用 Apache APISIX 默认配置（启用 Admin API，使用默认 Admin Key 且没有额外分配管理端口），攻击者可以通过 batch-requests 插件调用 Admin API 。

漏洞解决方案

iMC&U-Center1.0系列皆不涉及该漏洞