安全通告

关于 UI for Apache Kafka 后台 jmx jndi 存在代码执行漏洞的预警通报

发布日期：2024-7-18

[2024]014 号

漏洞描述

2024 年 7 月 18 日监测发现 UI for Apache Kafka 后台 jmx jndi 存在代码执行漏洞（CVE-2024-32030），该漏洞是由于在默认情况下 Kafka UI 未开启认证授权，攻击者可构造恶意请求利用后台功能执行任意代码，控制服务器。

Kafka UI 是 Apache Kafka 管理的开源 Web UI。Kafka UI API 允许用户通过指定网络地址和端口连接到不同的 Kafka brokers。作为一个独立的功能，它还提供了通过连接到其 JMX 端口监视 Kafka brokers 性能的能力。

漏洞编号

CVE-2024-32030

漏洞危害

攻击者可能利用这一漏洞设置一个恶意的 JMX 监听器，当 Kafka UI 尝试连接并获取监控数据时，攻击者可以发送一个恶意的序列化对象，导致 Kafka UI 执行远程代码。

漏洞等级

高危

受影响版本

Kafka UI <= 0.7.1

修复方案

目前官方已经发布了解决此漏洞的相关补丁，建议受影响用户升级至安全版本。

https://github.com/provectus/kafka-ui/releases/tag/v0.7.2

参考链接

https://securitylab.github.com/advisories/GHSL-2023-229_GHSL-2023-230_kafka-ui/

https://nvd.nist.gov/vuln/detail/CVE-2024-32030

https://github.com/provectus/kafka-ui/pull/4427