kafka-ui 存在远程命令执行漏洞

漏洞相关 吴昊A 2024-02-28 发表

漏洞相关信息

漏洞编号： 无
漏洞名称： kafka-ui 存在远程命令执行漏洞
产品型号及版本： COMWARE V7安全产品

漏洞描述

近日，国资国企在线监管安全运营中心（以下简称“安全 运营中心”）监测发现 kafka-ui 存在远程命令执行漏洞，严重 危害央企单位数据安全，目前已监测到攻击者利用该漏洞对中 央企业进行攻击。 请企业及时对部署的 kafka-ui（UI for Apache Kafka ） 进行排查，联系厂商获取修复方案，避免漏洞造成更大危害。 一、漏洞详情 kafka-ui 存在远程命令执行漏洞【高危】 影响：远程命令执行漏洞 UI for Apache Kafka 是一个免费的开源 Web UI，用于 监控和管理 Apache Kafka 集群。该应用存在远程命令执行漏 洞，攻击者可利用 “groovy”筛选器参数注入在服务器上执行 任意代码，从而窃取敏感数据信息。 二、影响范围 0.4.0≤kafka-ui ≤ 0.7.1 国资国企在线监管安全运营中心 - 2 - 三、修复建议 请各企业尽快联系厂商对漏洞进行修复。 https://docs.kafka-ui.provectus.io/overview/readme 临时整改建议： 1. 在安全设备上监测并阻断如下相关 URL 请求： 1）URL 请求“/api/clusters”获取 clusters name 的请 求。 2）URL 请求“/api/clusters/{上面的 clusters name}/t opics?showInternal=true”获取 topics name 的请求 。 3）URL 请求中包含“/api/clusters/local/topics/{上 面的 topic name}/messages?q=”关键词的请求。 2.如果没有紧急业务需求，在修复前避免将该系统暴露在 互联网侧或通过白名单限制访问。 3.如果在修复后需要配合验证，请联系中资网安。

漏洞解决方案

comware v7安全产品不涉及