

知 态势感知是否涉及WebLogic JNDI 注入远程代码执行漏洞

漏洞相关 王树岭 2023-04-23 发表

漏洞相关信息

漏洞编号: CVE-2023-21931

漏洞名称: WebLogic JNDI 注入远程代码执行漏洞

产品型号及版本: 态势感知系列

漏洞描述

漏洞编号

CVE-2023-21931

漏洞危害

远程攻击者在未授权情况下可通过构造特殊请求执行任意命令, 利用该漏洞获取控制权。

漏洞等级

高危

已验证受影响版本

WebLogic 12.2.1.3.0、12.2.1.4.0、14.1.1.0.0

修复方案

1. 官方修复措施

Oracle官方已发布修复方案, 建议及时更新。

<https://www.oracle.com/security-alerts/cpuapr2023.html>

2. 临时处置和应对措施

若非必须开启, 请禁用T3协议, 或者对协议端口进行严格的权限控制。

参考链接

- <https://www.oracle.com/security-alerts/cpuapr2023.html>

漏洞解决方案

态势感知不涉及

