防火墙，IPS，LB是否涉及WebLogic远程代码执行漏洞（CVE-2024-21181）

漏洞相关 **孔凡安** 4天前 发表

漏洞相关信息

漏洞编号： CVE-2024-21181
漏洞名称： Oracle WebLogic Server 存在远程代码执行漏洞
产品型号及版本： 产品型号及版本： Comware V5/V7/V9

漏洞描述

一、WebLogic远程代码执行漏洞自查及整改

Oracle WebLogic Server 存在远程代码执行漏洞，漏洞编号：CVE-2024-21181

1.影响版本

12.2.1.4.0和14.1.1.0.0

2.安全版本
除12.2.1.4.0和14.1.1.0.0之外的版本

3.处置建议

Oracle官方已经发布补丁修复了漏洞，Oracle官方更新链接如下：https://www.oracle.com/security-alerts/cpujul2024.html

4.处置建议
如非必要使用，建议禁用T3和IIOP协议，具体操作步骤如下：

a)禁用T3协议：

（1）进入WebLogic控制台，在base_domain的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。
（2）在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，在连接筛选器规则中输入：127.0.0.1 * * allow t3t3s，0.0.0.0/0 * *deny t3 t3s(t3和t3s协议的所有端口只允许本地访问)。
（3）保存后需重新启动，规则方可生效。

b)禁用IIOP协议：
在WebLogic控制台中，选择【环境】>>【服务器】>>点击【AdminServer（管理）】>>【协议】>>【IIOP】，取消勾选“启用IIOP”，保存并重启WebLogic项目。

漏洞解决方案

防火墙，IPS，LB不涉及Weblogic 组件，所以不涉及该漏洞。