WebLogic T3/IIOP 信息泄露漏洞（CVE-2024-21006/CVE-2024-21007）通告

■ 通告编号 **NS-2024-00015**	■ 发布日期 **2024-04-17**
■ 漏洞危害	**攻击者利用上述漏洞，可实现未授权访问。**
■ **TAG**	WebLogic、T3/IIOP、CVE-2024-21006、CVE-2024-21007

一. 漏洞概述

近日，绿盟科技 CERT 监测到 Oracle 发布安全公告，修复了 Oracle WebLogic Server 中存在的两个信息泄露漏洞（CVE-2024-21006/CVE-2024-21007），由于 T3/IIOP 协议存在缺陷，未经身份验证的攻击者可通过 T3/IIOP 协议受影响的服务器发送恶意的请求，访问目标系统上的敏感信息。请受影响的用户尽快采取措施进行防护。

WebLogic 是一款 Java EE 应用服务器，由 BEA 系统公司开发，现在归 Oracle 所有。它提供完整的 Java EE 平台和广泛的服务和功能，如 Web 服务器、EJB 容器、JMS 消息队列、事务管理、安全性等，并具有高度可扩展性和稳定性。

参考链接：

https://www.oracle.com/security-alerts/cpuapr2024.html

二. 影响范围

受影响版本

- WebLogic Server 12.2.1.4.0
- WebLogic Server 14.1.1.0.0

注：上述为目前 Oracle 官方仍支持维护的产品版本，10.3.6.0、11.1.1.9、12.1.3.0 等多个 WebLogic Server 旧版本已停止维护。

三. 漏洞检测

3.1 本地检测

可使用如下命令对 WebLogic 版本和补丁安装的情况进行排查。

```
$ cd /Oracle/Middleware/wlserver_10.3/server/lib
$ java -cp weblogic.jar    weblogic.version
```

在显示结果中，如果没有补丁安装的信息，则说明存在风险，如下图所示：

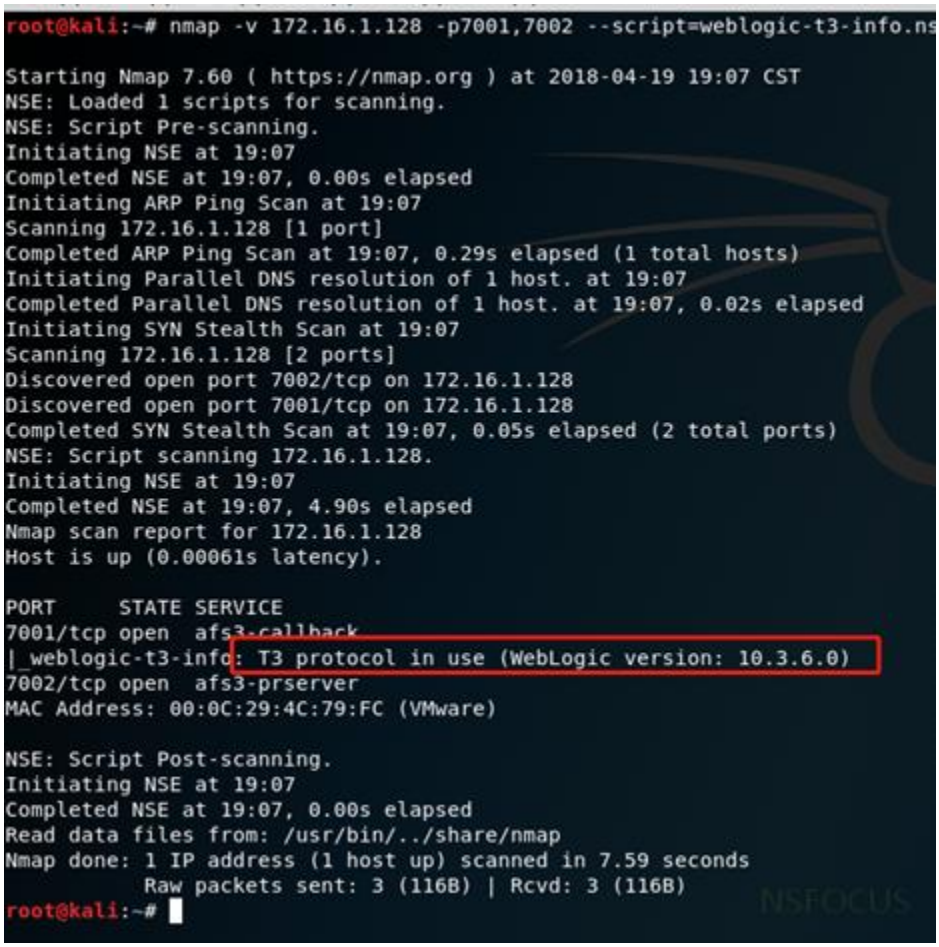
```
[root007@localhost lib]$ java -cp weblogic.jar weblogic.version

WebLogic Server 10.3.6.0  Tue Nov 15 08:52:36 PST 2011 1441050

Use 'weblogic.version -verbose' to get subsystem information

Use 'weblogic.utils.Versions' to get version information for all modules
[root007@localhost lib]$
```

3.2 T3 协议探测

Nmap 工具提供了 WebLogic T3 协议的扫描脚本，可探测开启 T3 服务的 WebLogic 主机。命令如下：

```
nmap -n -v -Pn  –sV [主机或网段地址] -p7001,7002 --script=weblogic-t3-info.nse
```

如下图红框所示，目标开启了 T3 协议且 WebLogic 版本在受影响范围之内，如果相关人员没有安装官方的安全补丁，则存在漏洞风险。



四. 漏洞防护

4.1 补丁更新

目前 Oracle 已发布补丁修复了上述漏洞，请用户参考官方通告及时下载受影响产品更新补丁，并参照补丁安装包中的 readme 文件进行安装更新，以保证长期有效的防护。下载链接：https://support.oracle.com/rs?type=doc&id=3011291.2

注：Oracle 官方补丁需要用户持有正版软件的许可账号，使用该账号登陆 https://login.oracle.com 后，可以下载最新补丁。

4.2 临时防护措施

如果用户暂时无法安装更新补丁，可通过下列措施进行临时防护：

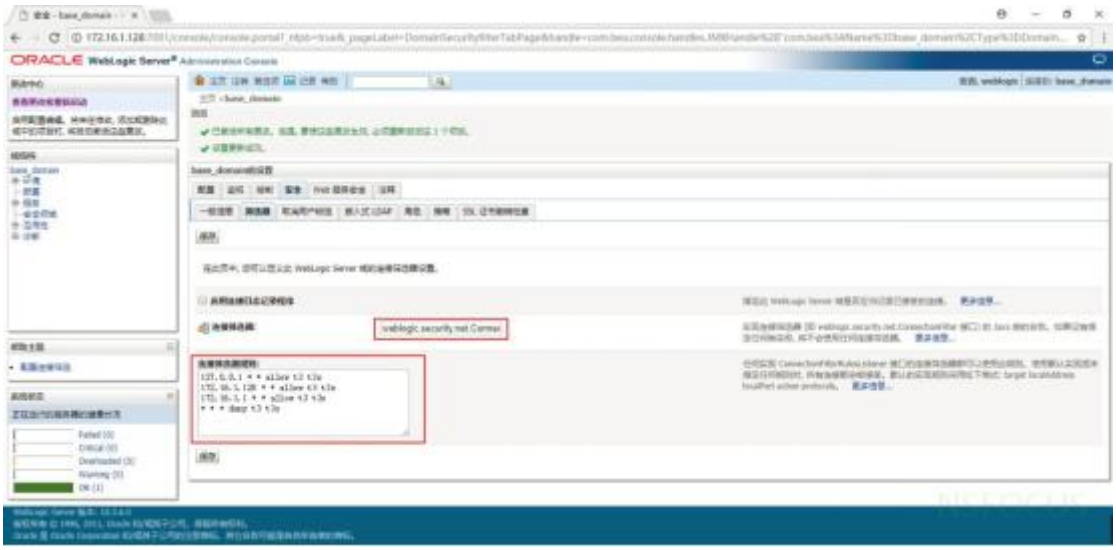
4.2.1 限制 T3 协议访问

用户可通过控制 T3 协议的访问来临时阻断针对利用 T3 协议漏洞的攻击。WebLogic Server 提供了名为 weblogic.security.net.ConnectionFilterImpl 的默认连接筛选器，此连接筛选器接受所有传入连接，可通过此连接筛选器配置规则，对 T3 及 T3s 协议进行访问控制，详细操作步骤如下：

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，参考以下写法，在连接筛选器规则中配置符合企业实际情况的规则：

```
127.0.0.1 * * allow t3 t3s

本机 IP ** allow t3 t3s

允许访问的 IP   * * allow t3 t3s

* * * deny t3 t3s
```

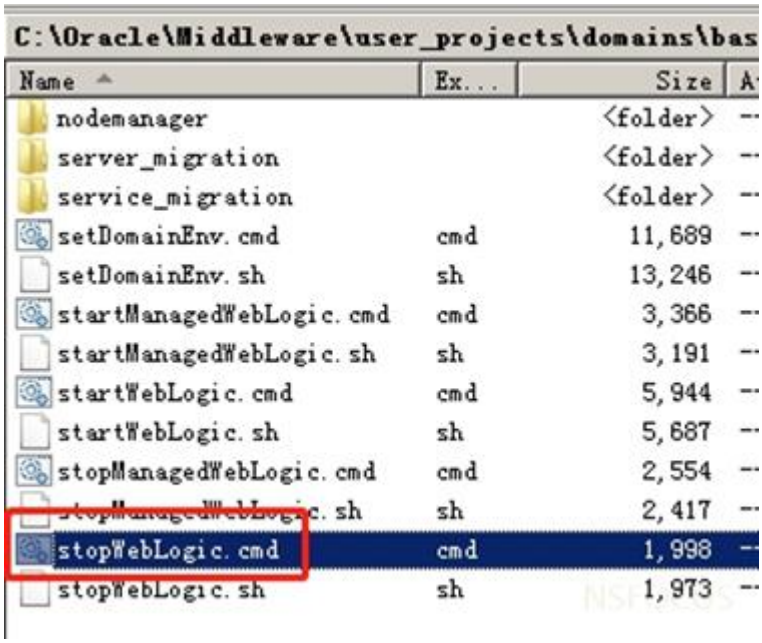


连接筛选器规则格式如下：target localAddress localPort action protocols，其中：

- target 指定一个或多个要筛选的服务器。
- localAddress 可定义服务器的主机地址。(如果指定为一个星号（*），则返回的匹配结果将是所有本地 IP 地址。)
- localPort 定义服务器正在监听的端口。(如果指定了星号，则匹配返回的结果将是服务器上所有可用的端口)。
- action 指定要执行的操作。(值必须为“allow”或“deny”。)
- protocols 是要进行匹配的协议名列表。(必须指定下列其中一个协议：http、https、t3、t3s、giop、giops、dcom 或 ftp。）如果未定义协议，则所有协议都将与一个规则匹配。

3. 保存后若规则未生效，建议重新启动 WebLogic 服务（重启 WebLogic 服务会导致业务中断，建议相关人员评估风险后，再进行操作）。以 Windows 环境为例，重启服务的步骤如下：

进入域所在目录下的 bin 目录，在 Windows 系统中运行 stopWebLogic.cmd 文件终止 WebLogic 服务，Linux 系统中则运行 stopWebLogic.sh 文件。



待终止脚本执行完成后，再运行 startWebLogic.cmd 或 startWebLogic.sh 文件启动 WebLogic，即可完成 WebLogic 服务重启。

4.2.2 禁用 IIOP 协议

用户可通过关闭 IIOP 协议阻断针对利用 IIOP 协议漏洞的攻击，操作如下：

在 WebLogic 控制台中，选择“服务”->“AdminServer”->“协议”，取消“启用 IIOP”的勾选。并重启 WebLogic 项目，使配置生效。

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。