

# 安全通告

## Oracle WebLogic Server 远程代码执行漏洞安全预警与建议

---

近日监测到 Oracle 官方发布安全通告，修复了一个 Oracle WebLogic Server 远程代码执行漏洞 (CVE-2023-21931)。这个漏洞源于 WebLogic 中 WLNamingManager 类的 getObjectInstance() 方法的缺陷。在默认设置下，未经授权的远程攻击者可以通过 T3/IIOP 协议传送特定对象，进而在目标系统上执行任意代码。

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。

### 一、影响范围

Weblogic 10.3.6

Weblogic 12.1.3

Weblogic 12.2.1.3.0

Weblogic 12.2.1.4.0

Weblogic 14.1.1.0.0

## 二、漏洞排查

### 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：

```
[root@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
[root@localhost lib]$
```

### 2. T3 协议检测

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：

```
root@kali:~# nmap -v 172.16.1.128 -p7001,7002 --script=weblogic-t3-info.nse

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-19 19:07 CST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:07
Completed NSE at 19:07, 0.00s elapsed
Initiating ARP Ping Scan at 19:07
Scanning 172.16.1.128 [1 port]
Completed ARP Ping Scan at 19:07, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:07
Completed Parallel DNS resolution of 1 host. at 19:07, 0.02s elapsed
Initiating SYN Stealth Scan at 19:07
Scanning 172.16.1.128 [2 ports]
Discovered open port 7002/tcp on 172.16.1.128
Discovered open port 7001/tcp on 172.16.1.128
Completed SYN Stealth Scan at 19:07, 0.05s elapsed (2 total ports)
NSE: Script scanning 172.16.1.128.
Initiating NSE at 19:07
Completed NSE at 19:07, 4.90s elapsed
Nmap scan report for 172.16.1.128
Host is up (0.00061s latency).

PORT      STATE SERVICE
7001/tcp  open  afs3-callback
|_weblogic-t3-info: T3 protocol in use (WebLogic version: 10.3.6.0)
7002/tcp  open  afs3-prserver
MAC Address: 00:0C:29:4C:79:FC (VMware)

NSE: Script Post-scanning.
Initiating NSE at 19:07
Completed NSE at 19:07, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
root@kali:~# █
```

## 三、漏洞防护

### 3. 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。

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

### 4. 临时防护措施

如果用户暂时无法安装更新补丁，可通过下列措施对高危漏洞进行临时防护：

#### 4.1 限制 T3 协议访问

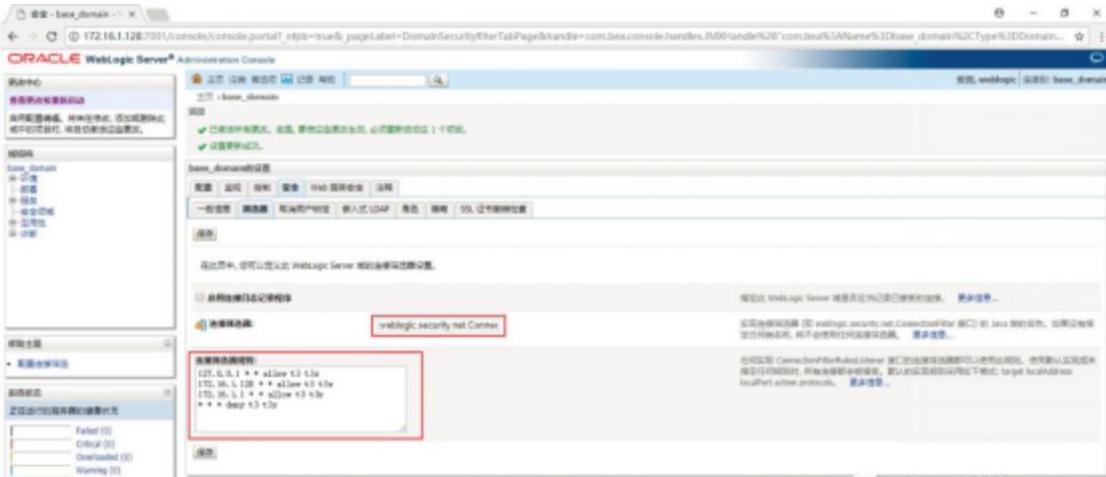
WebLogic Server 提供了名为 `weblogic.security.net.ConnectionFilterImpl` 的默认连接筛选器，此连接筛选器接受所有传入连接，可通过此连接筛选器配置规则，对 T3 及 T3s 协议进行访问控制，详细操作步骤如下：

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

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。

Name	Ex...	Size	A
nodemanager		<folder>	--
server_migration		<folder>	--
service_migration		<folder>	--
setDomainEnv.cmd	cmd	11,689	--
setDomainEnv.sh	sh	13,246	--
startManagedWebLogic.cmd	cmd	3,366	--
startManagedWebLogic.sh	sh	3,191	--
startWebLogic.cmd	cmd	5,944	--
startWebLogic.sh	sh	5,687	--
stopManagedWebLogic.cmd	cmd	2,554	--
stopManagedWebLogic.sh	sh	2,417	--
stopWebLogic.cmd	cmd	1,998	--
stopWebLogic.sh	sh	1,973	--

## 4.2 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。

