

【漏洞通告】Oracle WebLogic 服务器多个高危安全漏洞通告

1. 综述

WebLogic是美国Oracle公司出品的一个application server，确切的说是一个基于JAVAEE架构的中间件，WebLogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。

4月16日，Oracle官方发布了4月安全公告，披露WebLogic服务器存在多个高危漏洞，包括远程代码执行、任意文件上传、反序列化等。黑客利用漏洞可能可以远程获取WebLogic服务器权限，风险较大。

2. 漏洞概述

漏洞类型：远程代码执行、任意文件上传、反序列化

危险等级：高危

利用条件：Weblogic在受影响版本内

受影响范围：Weblogic 10.3.6.0、Weblogic 12.1.3.0、Weblogic 12.2.1.3

3. 漏洞编号

CVE-2019-2658、CVE-2019-2646、CVE-2019-2645、CVE-2019-1258、CVE-2019-2647、CVE-2019-2648、CVE-2019-2649、CVE-2019-2650、CVE-2019-2618、CVE-2019-2568、CVE-2019-2615

4. 漏洞描述

4月16日，Oracle官方发布了4月安全公告，披露WebLogic服务器存在多个高危漏洞，包括远程代码执行、任意文件上传、反序列化等。黑客利用漏洞可能可以远程获取WebLogic服务器权限，风险较大。

在4月16日的安全更新修复中，针对WebLogic的漏洞评级、影响概括如下：

漏洞编号	风险评级	CVSS 评分	影响协议
CVE-2019-2658	严重	9.8	HTTP
CVE-2019-2646	严重	9.8	T3
CVE-2019-2645	严重	9.8	T3
CVE-2019-1258	高危	7.5	HTTP
CVE-2019-2647	高危	7.5	HTTP
CVE-2019-2648	高危	7.5	HTTP
CVE-2019-2649	高危	7.5	HTTP
CVE-2019-2650	高危	7.5	HTTP
CVE-2019-2618	中危	5.5	HTTP
CVE-2019-2568	中危	5	HTTP
CVE-2019-2615	中危	4.9	HTTP

5.修复建议

安装官方补丁进行升级

下载地址：

<https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html>

临时修复建议：

1.关闭Weblogic T3服务

控制T3协议的访问

此漏洞产生于WebLogic的T3服务，因此可通过控制T3协议的访问来临时阻断针对该漏洞的攻击。当开放WebLogic控制台端口（默认为7001端口）时，T3服务会默认开启。

具体操作：

(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 t3 t3s, 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。

Administration Console

主页 注销 首选项 记录 帮助

主页 > base_domain

base_domain的设置

配置 监视 控制 安全 Web 服务安全 注释

一般信息 筛选器 取消用户锁定 嵌入式 LDAP 角色 策略 SSL 证书撤销检查

保存

在此页中, 您可以定义此 WebLogic Server 域的连接筛选器设置。

启用连接日志记录程序

连接筛选器: weblogic.security.net.(

连接筛选器规则:

```
127.0.0.1 ** allow t3 t3s, 0.0.0.0/0 ** deny t3 t3s
```

青藤实验室

2.检查Weblogic弱口令

排查Weblogic管理后台是否存在弱口令，增强密码强度。

6.即时检测

青藤云安全在漏洞爆出的第一时间，就已检测出该威胁并通知相关客户。

产品检查方法：登录青藤主机平台，选择资产清点——Web服务——Weblogic
服务名筛选出Weblogic服务，查看资产中的Weblogic是否在受影响版本内。

资产清点

Web 服务

业务组：所有 WebLogic X 版本：所有 启动用户：所有 配置文件路径：所有 二进制路径：所有

8 项

主机IP	Web服务名	版本	启动用户	二进制路径	配置文件路径
192.168.2.225	WebLogic	12.1.3.0.0	root	/usr/java/jdk...	/usr/local/wl...
192.168.72.128	WebLogic	12.1.3.0.0	root	/usr/lib/jvm/j...	/usr/local/op...
192.168.72.133	WebLogic	10.3.6.0	root	/usr/java/jdk...	/usr/local/op...
192.168.160.208	WebLogic	12.1.3.0.0	weblogic	/usr/java/jdk...	/home/myho...
192.168.192.111	WebLogic	10.3.6.0	root	/usr/java/jdk...	/usr/local/tes...
192.168.192.203	WebLogic	12.1.3.0.0	root	/usr/local/jav...	/root/wisnew...
192.168.197.205	WebLogic	10.3.6.0	root	/usr/java/jdk...	/usr/local/tes...
192.168.197.223	WebLogic	10.3.6.0	root	/usr/java/jdk...	/usr/local/tes...

青藤云安全

参考链接：

<https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html>

