WebLogic 一月份安全通告
安全通告

2021 年 1 月 21 日

目录

一、 漏洞概要 3
二、 漏洞分析 5
三、 影响范围 8
四、 解决方案 10

一、 漏洞概要

漏洞名称	Oracle 一月份高危漏洞安全公告
威胁等级	高危
影响范围	CVE-2021-2047 Oracle WebLogic Server 10.3.6.0.0 Oracle WebLogic Server 12.1.3.0.0 Oracle WebLogic Server 12.2.1.3.0 Oracle WebLogic Server 12.2.1.4.0 Oracle WebLogic Server 14.1.1.0.0 CVE-2021-2108 Oracle WebLogic Server 12.2.1.3.0 CVE-2021-1994 Oracle WebLogic Server 10.3.6.0.0 Oracle WebLogic Server 12.1.3.0.0 CVE-2021-2064 Oracle WebLogic Server 12.2.1.3.0 CVE-2021-2075 Oracle WebLogic Server 10.3.6.0.0 Oracle WebLogic Server 12.1.3.0.0 Oracle WebLogic Server 12.2.1.3.0 Oracle WebLogic Server 12.2.1.4.0 Oracle WebLogic Server 14.1.1.0.0

	CVE-2020-14756 Oracle WebLogic Server 3.7.1.0 Oracle WebLogic Server 12.1.3.0.0 Oracle WebLogic Server 12.2.1.3.0 Oracle WebLogic Server 12.2.1.4.0 Oracle WebLogic Server 14.1.1.0.0 CVE-2019-17195 Oracle WebLogic Server 12.2.1.3.0 Oracle WebLogic Server 12.2.1.4.0
利用难度	未知

二、 漏洞分析

2.1 组件介绍

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。

将 Java 的动态功能和 Java Enterprise 标准的安全性引入大型网络应用的开发、集成、部署和管理之中。WebLogic 是商业市场上主要的 Java（J2EE）应用服务器软件（application server）之一，是世界上第一个成功商业化的 J2EE 应用服务器，具有可扩展性，快速开发，灵活，可靠性等优势。

2.2 漏洞描述

Oracle 一月份发布的官方补丁通告中共发布了 329 个安全补丁，其中 Weblogic 组件的高危漏洞有 7 个，cvss 评分为 9.8，分别为 CVE-2021-2047、CVE-2021-2075、CVE-2021-2064、CVE-2021-1994、CVE-2021-2108、CVE-2020-14756、CVE-2019-17195。漏洞危害性较高，建议受影响的客户尽快更新官方发布的安全补丁。

CVE-2021-2047

该漏洞允许未经身份验证的攻击者通过 fasterxml 反序列化数据，攻击者成功利用此漏洞可以获得 Oracle WebLogic Server 权限。

CVE-2021-2075

该漏洞允许未经身份验证的攻击者通过 IIOP,T3 进行网络访问，未经身份验证的攻击者成功利用此漏洞可以获得 Oracle WebLogic Server 权限。

CVE-2021-2064

该漏洞允许未经身份验证的攻击者通过 IIOP,T3 进行网络访问，未经身份验证的攻击者成功利用此漏洞可以获得 Oracle WebLogic Server 权限。

CVE-2021-1994

该漏洞允许未经身份验证的攻击者通过 HTTP 进行网络访问，未经身份验证的攻击者成功利用此漏洞可以获得 Oracle WebLogic Server 权限。

CVE-2021-2108

该漏洞允许未经身份验证的攻击者通过 IIOP,T3 进行网络访问，未经身份验证的攻击者成功利用此漏洞可以获得 Oracle WebLogic Server 权限。

CVE-2020-14756

该漏洞允许未经身份验证的攻击者通过 IIOP,T3 进行网络访问，未经身份验证的攻击者成功利用此漏洞可以获得 Oracle WebLogic Server 权限。

CVE-2019-17195

该漏洞允许未经身份验证的攻击者通过 HTTP 进行网络访问，未经身份验证的攻击者成功利用此漏洞可以获得 Oracle WebLogic

Server 权限。

三、 影响范围

3.1. 目前受影响的 Weblogic 版本

CVE-2021-2047

Oracle WebLogic Server 10.3.6.0.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 12.2.1.3.0

Oracle WebLogic Server 12.2.1.4.0

Oracle WebLogic Server 14.1.1.0.0

CVE-2021-2108

Oracle WebLogic Server 12.2.1.3.0

CVE-2021-1994

Oracle WebLogic Server 10.3.6.0.0

Oracle WebLogic Server 12.1.3.0.0

CVE-2021-2064

Oracle WebLogic Server 12.2.1.3.0

CVE-2021-2075

Oracle WebLogic Server 10.3.6.0.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 12.2.1.3.0

Oracle WebLogic Server 12.2.1.4.0

Oracle WebLogic Server 14.1.1.0.0

CVE-2020-14756

Oracle WebLogic Server 3.7.1.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 12.2.1.3.0

Oracle WebLogic Server 12.2.1.4.0

Oracle WebLogic Server 14.1.1.0.0

CVE-2019-17195

Oracle WebLogic Server 12.2.1.3.0

Oracle WebLogic Server 12.2.1.4.0

四、 解决方案

4.1、官方解决方案

目前厂商已发布升级补丁修复漏洞，请受影响用户尽快进行升级加固。补丁获取链接：

https://www.oracle.com/security-alerts/cpujan2021.html

4.2、临时解决方案

(1) 可通过关闭 IIOP 协议对此漏洞进行临时防御

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。

(2) 对 T3 服务进行控制

在上图这个 WebLogic 界面中选择安全-筛选器，在下方出现的界面中找到“连接筛选器”，在里面输入 security.net.ConnectionFilterImpl，然后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，最后保存并重启服务器即可生效。