奇安信
新一代网络安全领军者

Oracle WebLogic Server

远程代码执行漏洞

安全风险通告

奇安信 CERT

2023 年 01 月 18 日

修订历史

时间	更新内容
2023 年 01 月 18 日	奇安信 CERT 监测到 Oracle WebLogic Server 远程代码执行漏洞，并成功分析复现此漏洞，创建初始报告。

目录

第1章 安全通告

尊敬的客户：

近日，奇安信 CERT 监测到 **Oracle WebLogic Server 远程代码执行漏洞(CVE-2023-21839)**，该漏洞允许未经身份验证的远程攻击者通过 T3/IIOP 协议网络访问并破坏易受攻击的 WebLogic 服务器，成功利用此漏洞可能导致 Oracle WebLogic 服务器被接管或敏感信息泄露。**奇安信 CERT 已第一时间分析复现此漏洞。鉴于该漏洞在低版本 JDK 环境下影响较大，建议客户尽快做好自查及安装补丁。**

奇安信 CERT 将持续关注该漏洞进展，并第一时间为您更新该漏洞信息。

第2章 漏洞信息

Oracle WebLogic Server 是一个统一的可扩展平台，用于在本地和云端开发、部署和运行企业应用程序，例如 Java。WebLogic Server 提供了 Java Enterprise Edition (EE)和 Jakarta EE 的可靠、成熟和可扩展的实现。

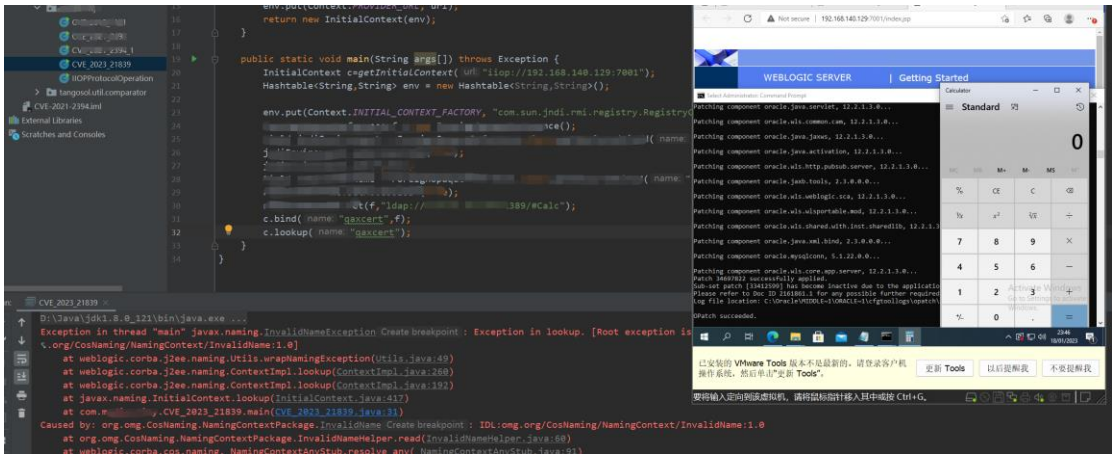
近日，奇安信 CERT 监测到 Oracle WebLogic Server 远程代码执行漏洞(CVE-2023-21839)，该漏洞允许未经身份验证的远程攻击者通过 T3/IIOP 协议网络访问并破坏易受攻击的 WebLogic 服务器，成功利用此漏洞可能导致 Oracle WebLogic 服务器被接管或敏感信息泄露。**奇安信 CERT 已第一时间分析复现此漏洞。**

鉴于该漏洞在低版本 JDK 环境下影响较大，建议客户尽快做好自查及安装补丁。

漏洞名称	**Oracle WebLogic Server 远程代码执行漏洞**		
公开时间	2023-01-18	**更新时间**	2023-01-18
CVE 编号	CVE-2023-21839	**其他编号**	QVD-2023-2423
威胁类型	代码执行	**技术类型**	反序列化错误
厂商	Oracle	**产品**	WebLogic Server
风险等级			
奇安信 CERT 风险评级		**风险等级**	
高危		蓝色（一般事件）	
现时威胁状态			
POC 状态	**EXP 状态**	**在野利用状态**	**技术细节状态**
未发现	未发现	已发现	未公开
漏洞描述	Oracle WebLogic Server 中存在远程代码执行漏洞，该漏洞允许未经身份验证的远程攻击者通过 T3/IIOP 协议网络访问并破坏易受攻击的 WebLogic 服务器，成功利用此漏洞可能导致 Oracle WebLogic 服务器被接管或敏感信息泄露。		

影响版本	Oracle WebLogic Server 12.2.1.3.0 Oracle WebLogic Server 12.2.1.4.0 Oracle WebLogic Server 14.1.1.0.0
其他受影响组件	无

目前，奇安信 CERT 已成功复现 **Oracle WebLogic Server 远程代码执行漏洞 (CVE-2023-21839)**，截图如下：



第3章 威胁评估

漏洞名称	Oracle WebLogic Server 远程代码执行漏洞		
CVE 编号	CVE-2023-21839	**其他编号**	QVD-2023-2423
CVSS 3.1 评级	高危	**CVSS 3.1 分数**	8.6
CVSS 向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	网络	低	
	所需权限（PR）	**用户交互（UI）**	
	无	不需要	
	影响范围（S）	**机密性影响（C）**	
	不改变	高	
	完整性影响（I）	**可用性影响（A）**	
	低	低	
危害描述	未授权的远程攻击者可通过 T3/IIOP 协议网络访问并破坏易受攻击的 WebLogic 服务器，成功利用此漏洞可能导致 Oracle WebLogic 服务器被接管或敏感信息泄露。		

第4章 处置建议

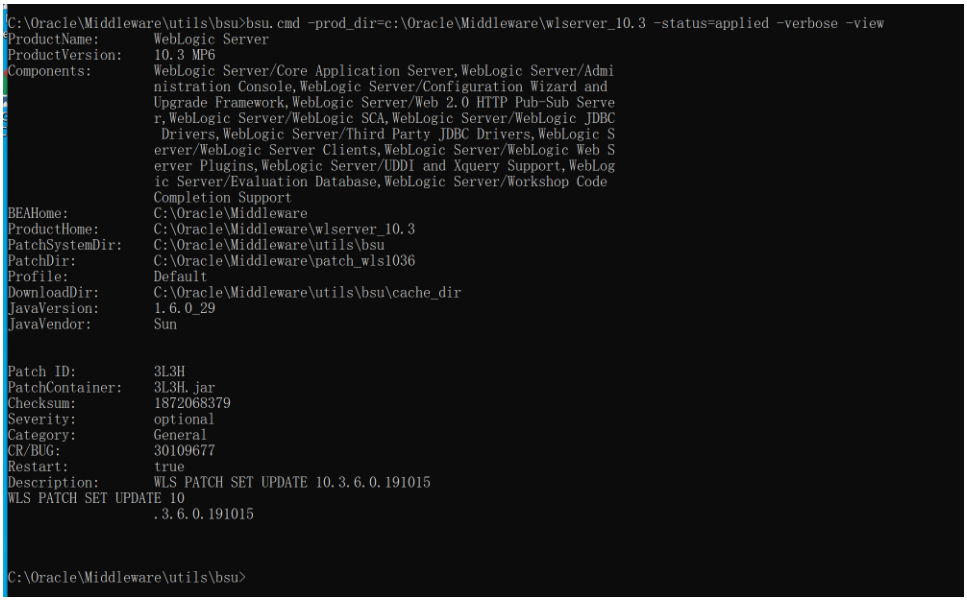
请参考以下链接安装补丁：

https://www.oracle.com/security-alerts/cpujan2023.html

Oracle WebLogic Server 升级方式

1. Oracle WebLogic Server 11g：

bsu.cmd -install -patch_download_dir=C:\Oracle\Middleware\utils\bsu\cache_dir -patchlist=3L3H -prod_dir=C:\Oracle\Middleware\wlserver_10.3

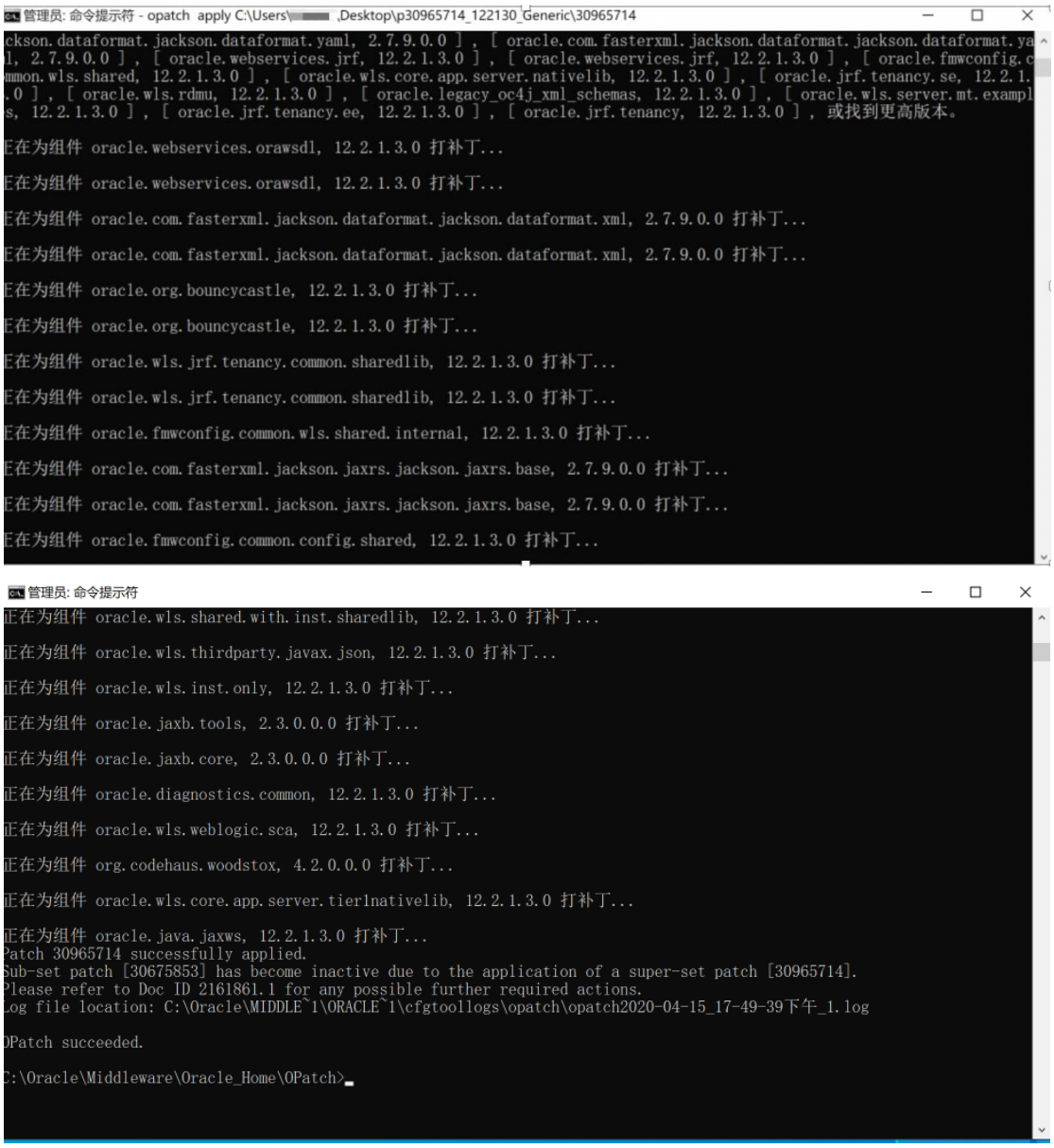


出现以上提示代表补丁安装成功。

2. Oracle WebLogic Server 12c：

使用 opatch apply 安装补丁

C:\Oracle\Middleware\Oracle_Home\OPatch>opatch apply 本机补丁地址



注：补丁编号请自行更改为新补丁编号。

若非必须开启，请禁用 T3 和 IIOP 协议。

禁用 T3、IIOP 协议具体操作步骤如下：

1. 禁用 T3:

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。

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。)

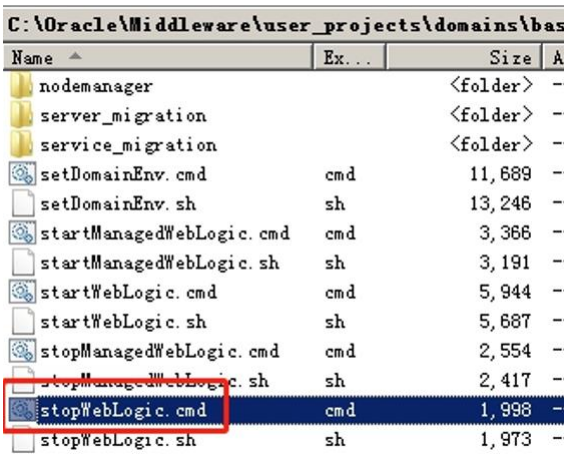
localPort 定义服务器正在监听的端口。(如果指定了星号，则匹配返回的结果将是服务器上所有可用的端口)。

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。

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。

2. 禁用 IIOP：

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。


ORACLE WebLogic Server® Administration Console
更改中心
查看更改和重新启动
启用配置编辑。将来在修改，添加或删除此域中的项目时，将自动激活这些更改。
域结构
base_domain
环境
部署
服务
安全领域
互用性
诊断
帮助主题
启用和配置 IIOP
配置定制网络通道
配置默认网络连接
系统状态
正在运行的服务器的健康状况
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
主页 注销 首选项 记录 帮助
欢迎, weblogic 连接到: base_domain
主页 >环境概要 >服务器概要 >AdminServer
消息
已激活所有更改。但是，要使这些更改生效，必须重新启动这 1 个项目。
设置更新成功。
AdminServer的设置
配置 协议 日志记录 调试 监视 控制 部署 服务 安全 注释
一般信息 HTTP jCOM IIOP 通道
保存
在此页中，您可以定义此服务器的 IIOP (Internet ORB 间协议) 设置。通过 IIOP，以不同编程语言编写的分布式程序可以通过 Internet 进行通信。
启用 IIOP
指定是否为此服务器的常规 (非 SSL) 和 SSL 端口都启用 IIOP 支持。 更多信息...
高级
保存

第5章 产品解决方案

5.1 奇安信天眼检测方案

奇安信天眼新一代安全感知系统已经能够有效检测针对该漏洞的攻击，请将规则版本升级到 3.0.0118.13713 或以上版本。规则 ID 及规则名称：0x5ea7，Weblogic 远程代码执行漏洞(CVE-2023-21839)。奇安信天眼流量探针规则升级方法：系统配置->设备升级->规则升级，选择“网络升级”或“本地升级”。

第6章 参考资料

[1] https://www.oracle.com/security-alerts/cpujan2023.html

奇安信 CERT

【我们是谁】

奇安信应急响应中心（奇安信 CERT）成立于 2016 年，隶属于奇安信旗下的威胁情报中心，旨在致力于向客户提供监测全面、响应迅速、认定客观、建议可行的漏洞情报。早在 Oracle 2020 年第二季度关键补丁更新公告中，就被评为了“在线状态安全性贡献者”。多次率先发现 WebLogic、Jackson 等知名软件和组件的高危漏洞并获得官方致谢。在风险通告方面，多次率先为客户提供漏洞和网络安全事件的风险通告、响应处置建议、相关技术分析和奇安信相关产品的解决方案。同时奇安信 CERT 在 Web 漏洞研究、二进制漏洞研究、前瞻性攻防工具预研等方面均积累了丰富的经验。

【我们的服务】

安全风险通告：奇安信 CERT 成立至今已发布上百篇安全风险通告，从成立至今，针对多个高危漏洞、网络安全事件发布风险通告并给出了有效的安全措施。我们的安全研究团队将实时跟踪安全热点事件和漏洞，始终站在用户的视角去评估风险，致力于第一时间向客户发送有效的风险和相关解决方案。

【订阅方式】

发送接收邮箱和所属单位至：

cert@qianxin.com

【微信公众号】

奇安信 CERT