安全漏洞通告

2021-04 补丁日: Oracle 多个产品漏洞安全风险通告

360CERT

360CERT
北京奇虎科技有限公司

报告信息

报告名称	2021-04 补丁日: Oracle 多个产品漏洞安全风险通告		
报告类型	安全漏洞通告	报告编号	B6-2021-042101
报告版本	1	报告日期	2021-04-21
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-04-21	360CERT	360CERT	撰写报告

目录

1 事件简述 3
2 风险等级 4
3 漏洞详情 5
Oracle Weblogic Server 多个严重漏洞 5
Oracle Communications Applications（Oracle 通信应用软件）多个严重漏洞 5
Oracle E-Business Suite（Oracle 电子商务套件）多个严重漏洞 6
Oracle Enterprise Manager（Oracle 企业管理软件）多个严重漏洞 6
Oracle Financial Services Applications（Oracle 金融服务应用软件）多个严重漏洞 7
4 修复建议 8
通用修补建议 8
临时修补建议 8
5 时间线 9
6 参考链接 10
附录 11
A 产品侧解决方案 11
360 安全分析响应平台 11
360 本地安全大脑 11
360 终端安全管理系统 12

1 事件简述

2021 年 04 月 21 日，360CERT 监测发现Oracle官方发布了2021年4月份的安全更新。此次安全更新发布了390个漏洞补丁，其中OracleFusionMiddleware有45个漏洞补丁更新，主要涵盖了OracleWeblogicServer、OracleOutsideInTechnology、OracleCoherence、OracleBusinessIntelligenceEnterpriseEdition等产品。在本次更新的45个漏洞补丁中，有36个漏洞无需身份验证即可远程利用。

对此，360CERT 建议广大用户好资产自查以及预防工作，以免遭受黑客攻击。

360CERT

2 风险等级

360CERT 对该事件的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

360CERT

3 漏洞详情

3.1 Oracle Weblogic Server 多个严重漏洞

Weblogic 本次更新了多个严重漏洞，这些漏洞允许未经身份验证的攻击者通过 IIOP 或 T3 协议发送构造好的恶意请求，从而在 Oracle WebLogic Server 执行代码或窃取关键数据。严重漏洞编号如下：

- CVE-2021-2136：未经身份验证的攻击者通过IIOP协议发送恶意请求，最终接管服务器，评分9.8
- CVE-2021-2135：未经身份验证的攻击者通过T3或IIOP协议发送恶意请求，最终接管服务器，评分9.8
- CVE-2021-2157：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终对关键数据进行未授权访问，评分7.5

3.2 Oracle Communications Applications（Oracle 通信应用软件）多个严重漏洞

此重要补丁更新包含针对OracleCommunicationsApplications的 13 个新的安全补丁。其中的 12 个漏洞无需身份验证即可远程利用，即可以通过网络利用而无需用户凭据。严重漏洞编号如下：

- CVE-2020-11612：未经身份验证的攻击者通过HTTP协议发送恶意请求，最终接管OracleCommunicationsDesignStudio，评分9.8
- CVE-2020-28052：未经身份验证的攻击者通过HTTPS协议发送恶意请求，最终接管OracleCommunicationsMessagingServer，评分9.8
- CVE-2020-5421：未经身份验证的攻击者通过HTTPS协议发送恶意请求，最终接管OracleCommunicationsUnifiedInventoryManagement，评分8.8

3.3 Oracle E-Business Suite（Oracle 电子商务套件）多个严重漏洞

此重要补丁更新包含针对OracleE-BusinessSuite的 70 个新的安全补丁。其中的 22 个漏洞无需身份验证即可被远程利用，即可以在不需要用户凭据的情况下通过网络利用这些漏洞。严重漏洞编号如下：

- CVE-2021-2200：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终对关键数据进行未授权访问，评分9.1
- CVE-2021-2205：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终对关键数据进行未授权访问，评分9.1
- CVE-2021-2209：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终对关键数据进行未授权访问，评分8.5

3.4 Oracle Enterprise Manager（Oracle 企业管理软件）多个严重漏洞

此重要补丁更新包含针对OracleEnterpriseManager的 9 个新的安全补丁。其中的 8 个漏洞无需身份验证即可远程利用，即可以通过网络利用而无需用户凭据。严重漏洞编号如下：

- CVE-2019-17195：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终接管企业管理器基础平台，评分9.8
- CVE-2019-5064：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终接管 Oracle 应用测试套件，评分8.8
- CVE-2020-10878：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终对关键数据进行未授权访问，评分8.6

3.5 Oracle Financial Services Applications（Oracle 金融服务应用软件）多个严重漏洞

此重要补丁更新包含针对OracleFinancialServicesApplications的 15 个新的安全补丁。其中的 10 个漏洞无需身份验证即可远程利用，即可以在不需要用户凭据的情况下通过网络利用这些漏洞。严重漏洞编号如下：

- CVE-2020-11998：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终接管Oracle FLEXCUBE 私人银行业务，评分9.8
- CVE-2020-5413：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终接管Oracle FLEXCUBE 私人银行业务，评分9.8
- CVE-2019-3773：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终接管Oracle FLEXCUBE 私人银行业务，评分9.8
- CVE-2019-17638：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终对关键数据进行未授权访问及拒绝服务攻击，评分9.4
- CVE-2020-26217：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终接管金融服务应用程序，评分8.8
- CVE-2020-5421：未经身份验证的攻击者可以通过HTTP发送恶意请求，最终接管Oracle FLEXCUBE 私人银行业务，评分8.8

4 修复建议

4.1 通用修补建议

及时更新补丁，参考 oracle 官网发布的补丁:Oracle Critical Patch Update Advisory - April 2021。

4.2 临时修补建议

1. 如果不依赖 T3 协议进行 JVM 通信，禁用 T3 协议：
- 进入 WebLogic 控制台，在 base_domain 配置页面中，进入安全选项卡页面，点击筛选器，配置筛选器。
- 在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，在连接筛选器规则框中输入 7001 deny t3 t3s 保存生效。
- 重启 Weblogic 项目，使配置生效。
2. 如果不依赖 IIOP 协议进行 JVM 通信，禁用 IIOP 协议：
- 进入 WebLogic 控制台，在 base_domain 配置页面中，进入安全选项卡页面。
- 选择"服务"->"AdminServer"->"协议"，取消"启用 IIOP"的勾选。
- 重启 Weblogic 项目，使配置生效。

5 时间线

2021-04-20 Oracle 发布安全更新通告

2021-04-21 360CERT 发布通告

360CERT

6 参考链接

Oracle Critical Patch Update Advisory - April 2021

360CERT

A 产品侧解决方案

A.1 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn) 获取对应产品。

A.2 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

A.3 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。