安全漏洞通告

2021-07 补丁日: Oracle 多个产品漏洞安全风险通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	2021-07 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	B6-2021-072101
报告版本	1	报告日期	2021-07-21
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	2021-07-21	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 07 月 21 日，360CERT 监测发现 Oracle官方 发布了 2021年7月份 的安全更新。

此次安全更新发布了342个漏洞补丁，其中OracleFusionMiddleware有48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48个漏洞补丁中，有35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。

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
攻击者价值	高
利用难度	低
360CERT 评分	9.8

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-2021-2394：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-2021-2397：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-2021-2382：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

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 33 个新的安全补丁。其中的 22 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-2021-21345：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OracleCommunicationsBRM-ElasticChargingEngine，评分9.9
- 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OracleCommunicationsBRM-ElasticChargingEngine，评分9.8
- CVE-2021-3177：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OracleCommunicationsOfflineMediationController，评分9.8
- CVE-2020-17530：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OracleCommunicationsPricingDesignCenter，评分9.8

- CVE-2019-17195：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OracleCommunicationsPricingDesignCenter，评分9.8

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 17 个新的安全补丁。其中的 3 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-2021-2355：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-2021-2436：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8.2
- CVE-2021-2359：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8.2

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 8 个新的安全补丁。全部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-2020-10683：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，最终接管企业管理器基础平台，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 22 个新的安全补丁。其中的 17 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-2021-21345：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 银行企业默认管理，评分9.9
- CVE-2019-0228：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 银行流动性管理，评分9.8
- CVE-2021-26117：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-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-2020-27218：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

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 - July 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

2021-07-20 Oracle 发布安全更新通告

2021-07-21 360CERT 发布通告

6 参考链接

Oracle Critical Patch Update Advisory - July 2021

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

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。

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。

B 报告等级说明

360CERT 评分是依托于 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 实施攻击成本低，难度低 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 (a) 占用存储空间 (b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

C 影响面说明

影响面说明	
广泛	1. 影响主体数 > 10w 2. 底层依赖库
一般	1. 5w < 影响主体数 < 10w 2. 次级开源库
局限	1. 影响主体数 < 5w 2. 特制版本的

D 360CERT 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 –10.0	严重
7.0 –8.9	高危
4.0 –6.9	中危
0 –3.9	低危