安全事件通告

2020-10 补丁日:Oracle 多个产品高危漏洞安全风险通告

360CERT
北京奇虎科技有限公司 | 2020-10-21

报告信息

报告名称	2020-10 补丁日:Oracle 多个产品高危漏洞安全风险通告		
报告类型	安全事件通告	**报告编号**	B6-2020-102101
报告版本	1	**报告日期**	2020-10-21
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2020-10-21	360CERT	360CERT	撰写报告

目录

一、 事件档案

漏洞类型	代码执行漏洞
CVE 编号	多个
相关厂商	Oracle
相关组件	多个
威胁等级	严重
影响面	广泛
360CERT 评分	10
修复方案	通用修补方案/临时修补方案
事件发布时间	2020-10-21
报告生成时间	2020-10-21

二、事件简述

2020 年 10 月 21 日，360CERT 监测发现 Oracle 官方 发布了 10 月份 的安全更新。

此次安全更新发布了 421 个漏洞补丁，其中 Oracle Fusion Middleware 有 46 个漏洞补丁更新，主要涵盖了 Oracle Weblogic、Oracle Endeca Information Discovery Integrator、Oracle WebCenter Portal、Oracle BI Publisher、Oracle Business Intelligence Enterprise Edition 等产品。在本次更新的 46 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 建议广大用户及时安装最新补丁，做好资产自查以及预防工作，以免遭受黑客攻击。

三、 事件评级

经过安全技术人员的分析，最终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	10

四、 事件详情

Oracle MySQL

此重要补丁更新包含 54 个针对 Oracle MySQL 的新安全补丁。其中的 4 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-2020-8174

Oracle Database Server

此重要补丁更新包含针对 Oracle 数据库服务器 的 30 个新安全补丁。这些漏洞中的 4 个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-2020-14735
- CVE-2020-14734

Oracle WebLogic Server 多个反序列化漏洞

Weblogic 本次更新了多个反序列化漏洞，这些漏洞允许未经身份验证的攻击者通过 HTTP、IIOP、T3 协议发送构造好的恶意请求，从而在 Oracle WebLogic Server 执行代码。严重漏洞编号如下：

- CVE-2020-14882
- CVE-2020-14841
- CVE-2020-14825

- CVE-2020-14859
- CVE-2020-14820

其中成功利用 CVE-2020-14882 漏洞的远程攻击者可以构造特殊的 HTTP 请求，在未经身份验证的情况下接管 WebLogic Server ，并在 WebLogic Server 执行任意代码。

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

此重要补丁更新包含针对 Oracle Communications 的 52 个新的安全补丁。其中的 41 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-2020-10683
- CVE-2020-11973
- CVE-2020-2555
- CVE-2020-11984

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 Oracle E-Business Suite 的 27 个新的安全补丁。其中的 25 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-2020-14855
- CVE-2020-14805

- CVE-2020-14875
- CVE-2020-14876

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 Oracle Enterprise Manager 的 11 个新安全补丁。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-2019-13990
- CVE-2018-11058
- CVE-2019-17638
- CVE-2020-5398
- CVE-2020-1967

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 Oracle Financial Services 应用程序的 53 个新的安全补丁。其中的 49 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-2019-17495
- CVE-2019-10173
- CVE-2020-10683

- CVE-2020-9546
- CVE-2020-11973
- CVE-2020-14824

五、 安全建议

(一) 通用修补方案

及时更新补丁，参考 oracle 官网发布的补丁:Oracle Critical Patch Update Advisory - October 2020:

https://www.oracle.com/security-alerts/cpuoct2020traditional.html

(二) 临时修补方案

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。

六、 产品侧解决方案

(一) 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台(quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。

(二) 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。

七、 参考链接

1. Oracle Critical Patch Update Advisory - October 2020

   https://www.oracle.com/security-alerts/cpuoct2020traditional.html

附录 A 报告风险等级说明

360CERT 评分是依托 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. 任意攻击者可直接发起攻击 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

附录 B 影响面说明

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

附录 C 360 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