Oracle 发布 2025 年 7 月的安全公告

2025-07-18 15:43:45

安全公告编号:CNTA-2025-0011

2025 年 7 月 15 日，Oracle 发布了 2025 年 7 月份的安全更新，修复了其多款产品存在的 309 个安全漏洞。受影响的产品包括：Oracle Database Server 数据库（6 个）、Oracle Application Express（1 个）、Oracle Blockchain Platform（1 个）、Oracle GoldenGate（5 个）、Oracle NoSQL Database（1 个）、Oracle REST Data Services（1 个）、Oracle Commerce（1 个）、Oracle Communications Applications（29 个）、Oracle Communications（84 个）、Oracle Construction and Engineering（2 个）、电子商务套装软件 Oracle E-Business Suite（9 个）、Oracle Enterprise Manager（1 个）、Oracle Financial Services Applications（18 个）、中间件产品 Fusion Middleware（36 个）、Oracle Analytics（5 个）、Oracle HealthCare Applications（3 个）、Oracle Hospitality Applications（1 个）、Oracle Hyperion（4 个）、Oracle Insurance Applications（3 个）、Oracle Java SE（11 个）、Oracle JD Edwards（2 个）、Oracle MySQL 数据库（40 个）、Oracle PeopleSoft（7 个）、Oracle Retail Applications（11 个）、Oracle Siebel CRM（6 个）、Oracle Supply Chain（8 个）、Oracle Utilities Applications（6 个）和 Oracle Virtualization（7 个）。

本次安全更新涉及的漏洞中，共包括 153 个高危漏洞，260 个可被远程利用漏洞。值得关注的漏洞情况如下表所示。CNVD 提醒广大 Oracle 用户，请及时下载补丁更新，避免引发漏洞相关的安全事件。

CVE 编号	公告标题和摘要	最高严重等级	受影响的软件
CVE-2025-30762	**Oracle WebLogic Server 未授权访问漏洞**	重要	Oracle WebLogic Server 12.2.1.

	由于 Oracle WebLogic Server 对通过 T3/IIOP 协议传入的数据缺乏充分鉴权与过滤，未经授权的远程攻击者无需任何凭据，仅通过向目标 WebLogic 实例发送特制的 T3 或 IIOP 报文，即可绕过身份验证逻辑，直接读取服务器可访问的全部关键数据。		4.0 Oracle WebLogic Server 14.1.1.0.0 Oracle WebLogic Server 14.1.2.0.0
CVE-2025-30753	**Oracle WebLogic Server 拒绝服务漏洞** Oracle WebLogic Server 在解析并处理特定 HTTP 请求时对资源消耗缺乏有效限制，低权限攻击者可利用此缺陷远程触发无限循环或内存/线程资源耗尽，使进程挂起或频繁崩溃。	次要	Oracle WebLogic Server 12.2.1.4.0 Oracle WebLogic Server 14.1.1.0.0 Oracle WebLogic Server 14.1.2.0.0

参考信息：

https://www.oracle.com/security-alerts/cpujul2025.html

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由国家计算机网络应急技术处理协调中心（中文简称国家互联应急中心，英文简称 CNCERT）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库。

在发布漏洞公告信息之前，CNVD 都力争保证每条公告的准确性和可靠性。然而，采纳和实施公告中的建议则完全由用户自己决定，其可能引起的问题和结 果也完全由用户承担。是否采纳我们的建议取决于您个人或您企业的决策，您应考虑其内容是否符合您个人或您企业的安全策略和流程。

我们鼓励所有计算机与网络安全研究机构，包括厂商和科研院所，向我们报告贵单位所发现的漏洞信息。我们将对所有漏洞信息进行验证并在 CNCERT/CC 网站和国家信息安全漏洞共享平台（CNVD）公布漏洞信息及指导受影响用户采取措施以避免损失。