Weblogic Server 高危远程代码执行漏洞的风险提示

2020 年 1 月 15 日，Oracle 官方发布 2020 年 1 月关键补丁更新公告 CPU（Critical Patch Update），其中 CVE-2020-2551 和 CVE-2020-2546 涉及 WebLogic Server 核心组件，影响面较大。这两个漏洞均在 WebLogic Server 默认配置下即可触发，无需管理员身份认证及额外交互，攻击者即可通过远程执行命令接管服务器，读取敏感信息等。针对 CVE-2020-2551，Oracle 官方目前只发布了部分版本的补丁，对于 CVE-2020-2546 尚未有官方补丁。如使用了 Oracle WebLogic 组件，需要及时应对处置，及时下载官方补丁程序并安装更新。在补丁未发布期间，要尽快采取缓解措施。

一、影响范围

CVE-2020-2551 影响版本：

- Oracle WebLogic Server 10.3.6.0.0（目前无官方补丁）
- Oracle WebLogic Server 12.1.3.0.0（目前无官方补丁）
- Oracle WebLogic Server 12.2.1.3.0（已发布官方补丁）
- Oracle WebLogic Server 12.2.1.4.0（已发布官方补丁）

CVE-2020-2546 影响版本：

- OracleWebLogicServer 10.3.6.0.0（目前无官方补丁）
- OracleWebLogicServer 12.1.3.0.0（目前无官方补丁）

二、触发条件

CVE-2020-2551

- WebLogic 默认启用 IIOP 协议
- 漏洞触发无需身份认证

CVE-2020-2546

- WebLogic 默认启用 T3 协议
- 漏洞触发无需身份认证

三、缓解措施

1.针对 CVE-2020-2551，用户可通过关闭 IIOP 协议对此漏洞进行缓解。操作如下：进入 WebLogic 控制台，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。

2.针对 CVE-2020-2546，用户可通过临时禁用 T3 协议连接对此漏洞进行缓解。操作如下：进入 WebLogic 控制台，在 base_domain 配置页面中，进入“安全选项卡”->“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” 并重启 Weblogic 项目，使配置生效。

官方公告链接：https://www.oracle.com/security-alerts/cpujan2020.html