Weblogic 远程代码执行漏洞(CVE-2018-3245)

威胁预警通告

北京时间 10 月 17 日凌晨，Oracle 官方发布了 10 月份（第三季度）关键补丁更新 CPU（CriticalPatchUpdate）,其中修复了一个 7 月份（第二季度）CPU 补丁中未能完全修复的（CVE-2018-2893）Weblogic 远程代码执行漏洞，此次新修复的漏洞编号为 CVE-2018-3245。

漏洞概述

WebLogic 是美国 Oracle 公司出品的一个 applicationserver，是一个基于 JAVAEE 架构的中间件，WebLogic 是用于开发、集成、部署和管理大型分布式 Web 应用、网络应用和数据库应用的 Java 应用服务器。

OracleWebLogicServer 存在远程代码执行漏洞。该漏洞通过 JRMP 协议利用 RMI 机制的缺陷达到执行任意反序列化代码的目的。攻击者可以在未授权的情况下将 payload 封装在 T3 协议中，通过对 T3 协议中的 payload 进行反序列化，从而实现对存在漏洞的 WebLogic 组件进行远程攻击，执行任意代码并可获取目标系统的所有权限。

漏洞危害

通过该漏洞攻击者可以在未授权的情况下远程执行任意代码。

漏洞影响版本

Weblogic10.3.6.0

Weblogic12.1.3.0

Weblogic12.2.1.3

解决方案

Oracle 官方已经在本次的关键补丁更新（CPU）中修复了该漏洞，强烈建议受影响的用户尽快升级更新进行防护。

注：Oracle 官方补丁需要用户持有正版软件的许可账号，使用该账号登陆 https://support.oracle.com 后，可以下载最新补丁。