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-

3 245 。

漏洞概 述

W ebL ogic 是美国 Oracle 公司出品的一个 applicationse rve r，是

一个基于 J AVA EE 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 J ava 应用服

务器。

O rac leW ebL ogicServer 存在远程代码执行漏洞。该漏洞通过 JRMP

协议利用 R MI 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 pay loa d 封装在 T3 补丁

溿⅀伐đ腖‰ 䀀

1

1

>•1

北京时间

>•1

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。