山西省互联网网络安全预警信息通报

山西省通信管理局
主办：国家计算机网络应急技术处理协调中心山西分中心　2019 年 6 月 15 日

关于 Oracle WebLogic 远程命令执行 0day（CVE-2019-2725 补丁绕过）漏洞的安全公告

近日，深信服安全团队发现了 Oracle WebLogic 远程命令执行 0day（CVE-2019-2725 补丁绕过）漏洞，该漏洞是由于应用在处理反序列化输入信息时存在缺陷，攻击者可以通过发送精心构造的恶意 HTTP 请求，获得目标服务器的权限，并在未授权的情况下执行远程命令，最终获取服务器的权限。

一、漏洞情况分析

该漏洞的利用方式与官方 4 月修复的 CVE-2019-2725 漏洞利用方式极为相似，属于 CVE-2019-2725 漏洞的变形绕过，所以攻击可以绕过官方四月份发布的安全补丁，且该漏洞是由于应用在处理反序列化输入信息时存在缺陷，攻击者

可以通过发送精心构造的恶意 HTTP 请求，用于获得目标服务器的权限，并在未授权的情况下执行远程命令，最终获取服务器的权限。

对上述漏洞的综合评级为“高危”。

二、漏洞影响范围

JDK<=1.6 且 Oracle WebLogic Server <= 10.3.6.0

三、处置措施

由于官方暂未发布补丁，建议通过以下临时解决措施来化解漏洞导致风险:

1.建议客户针对服务器使用情况，删除以下两个文件并重启 Weblogic 服务:

wls9_async_response.war 文件及相关文件夹

wls-wsat.war 文件及相关文件夹

文件路径如下:

10.3.*版本:

\Middleware\wlserver_10.3\server\lib\%DOMAIN_HOME%\servers\AdminServer\tmp_WL_internal\%DOMAIN_HOME%\servers\AdminServer\tmp\.internal\

12.1.3 版本:

\Middleware\Oracle_Home\oracle_common\modules\%DOMAIN_HOME%\servers\AdminServer\tmp\.internal\%DOMAIN_HOME%\servers\AdminServer\tmp_WL_internal\

2.通过访问限制配置来限制访问/_async/* 路径的请求。

3.及时升级Weblogic中的Java版本。