【漏洞通告】Oracle WebLogic wls9-async反序列化远程命令执行漏洞通告

近日，青藤实验室监测到多家用户出现了利用WebLogic wls9-async反序列化进行挖矿的入侵事件，其主要体征为系统负载升高。用户运行的weblogic服务存在最新的weblogic反序列化漏洞，被成功利用后进行挖矿程序的下载与执行，从而进行虚拟货币的挖取，进而获取利益。

1.综述

WebLogic是美国Oracle公司出品的一个application server，确切的说是一个基于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。

WebLogic wls9_async_response 包在反序列化处理输入信息时存在缺陷，攻击者可以发送精心构造的恶意 HTTP 请求，获得目标服务器的权限，在未授权的情况下远程执行命令。部分版本WebLogic中默认包含此WAR包，主要是为WebLogic Server提供异步通讯服务。

2.漏洞概述

漏洞类型：反序列化远程命令执行

危险等级：高危

利用条件：Weblogic在受影响版本内

受影响范围：WebLogic 10.3.6.0.0，12.1.3.0.0，12.2.1.1.0，12.2.1.2.0

3.漏洞编号

CNVD-C-2019-48814

4.漏洞描述

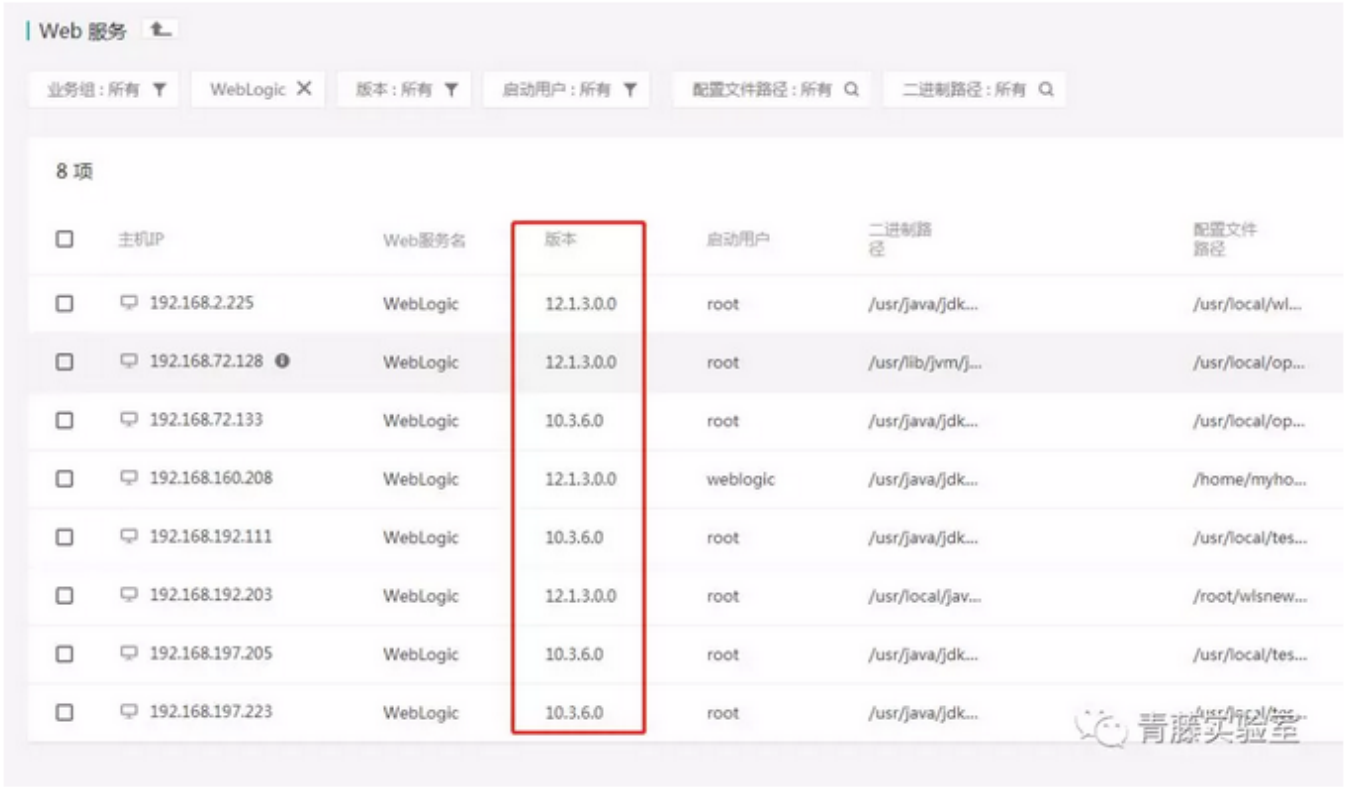
WebLogic wls9_async_response 包在反序列化处理输入信息时存在缺陷，攻击者可以发送精心构造的恶意 HTTP 请求，获得目标服务器的权限，在未授权的情况下远程执行命令。部分版本WebLogic中默认包含此WAR包，主要是为WebLogic Server提供异步通讯服务。

5.修复建议

官方暂未发布补丁，临时解决方案如下：
(1) 删除wls9_async_response的war包并重启webLogic，具体路径如下：
Weblogic 10 版本：
/%WLS_HOME%/wlserver_10.3/server/lib/bea_wls9_async_response.war
Weblogic 12 版本：
/%WLS_HOME%/oracle_common/modules/com.oracle.webservices.wls.bea-wls9-async-response_12.1.3.war
(2) 通过访问策略控制禁止 /_async/* 路径的URL访问。

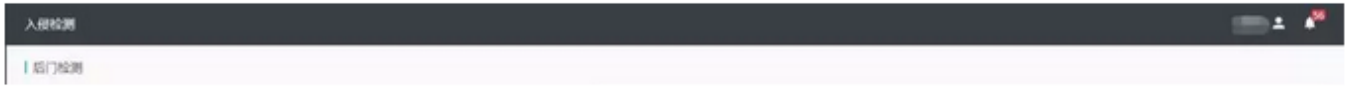
6.即时检测

登录青藤主机平台，选择资产清点—分级视图—Web服务—Weblogic
服务名筛选出Weblogic服务，查看资产中的Weblogic主机分布和版本情况。



在 WebLogic 地址加入目录：/_async 和 /_async/AsyncResponseService ，测试是否启用该组件，如果能访问则说明启用 wls9_async 组件，则存在漏洞。

PS：相关后门可通过入侵检测—后门检测，查看是否存在。



参考链接：

http://www.cnvd.org.cn/webinfo/show/4989

https://mp.weixin.qq.com/s/DyEn1p1KUX2HILfk6wMJ3w