TLP:WHITE

金融資安資訊分享與分析中心

弱點公告

Oracle WebLogic Server zero-day 漏洞公告

發行日期：2019 年 4 月 26 日

TLP:WHITE

中國資安公司於 2019/04/21 發布 Oracle WebLogic Server 之 zero-day 漏洞，目前 Oracle 公司尚未發布修正程式，請使用相關產品之單位盡速設定緩解措施。

〔TLP：WHITE〕

概述

中國資安公司 KnownSec 404 Team 於 4/21 發布 WebLogic Server 反序列化漏洞，攻擊者成功利用此漏洞將可遠端執行程式碼。

漏洞原因為 Oracle WebLogic Server 中的 wls9_async 及 wls-wsat 元件中可被觸發反序列化遠端程式碼執行。於所有 WebLogic 版本(包括最新版本)上執行 wls9_async_response.war 及 wls-wsat.war 元件時，即可利用此漏洞。

wls9-async 組件為 WebLogic Server 提供非同步通信服務，WebLogic 部分版本上預設為啟用。由於 WAR 包在反序列化輸入信息方面存在缺陷，因此攻擊者可以通過發送特製的惡意 HTTP 請求來獲取目標伺服器的權限，並在未經授權的情況下遠端執行指令。

Oracle 公司尚未針對此漏洞發布修正程式。

TLP:WHITE

此漏洞尚無 CVE 編號

影響版本/型號:

WebLogic 10.X

WebLogic 12.1.3

緩解措施

1. 找到並刪除 wls9_async_response.war 及 wls-wsat.war 元件程式，之後重啟 WebLogic 伺服器。
2. 限制 URL 存取。於防護設備 (例如 WAF) 設定存取規則，禁止以 URL 連至/_async/*及/wls-wsat/* 等路徑。

Temporary Solution

Scenario-1: Find and delete wls9_async_response.war, wls-wsat.war and restart the Weblogic service

Scenario-2: Controls URL access for the /_async/* and /wls-wsat/* paths by access policy control.

.

參考連結

1. https://medium.com/@knownseczoomeye/knownsec-404-

TLP:WHITE

team-oracle-weblogic-deserialization-rce-vulnerability-0day-alert-90dd9a79ae93