TLP:WHITE

金融資安資訊分享與分析中心

弱點公告-1080117-1

(Oracle 公告 2019 年 1 月安全性更新)

發行日期：2019 年 01 月 17 日

TLP:WHITE

摘要:

Oracle 於 2019 年 1 月 15 日(美國時間)發布了多項產品安全更新，本次於 Oracle Database Server、Oracle Fusion Middleware 及 MySQL 新發現的漏洞中，有 5 項之 CVSS 3.0 分數大於 7.0，屬於高風險。以下將分別說明各漏洞產生原因、影響範圍及修補方式。

漏洞說明：

項次一、CVE-2019-2406

概述：

Oracle Database Server 的核心 RDBMS(Relational Database Management System)元件存在漏洞。
高權限的攻擊者可輕易利用此漏洞，建立連線及執行目錄角色權限，藉由 Oracle Net 進行網路存取以入侵核心 RDBMS。
成功利用此漏洞之攻擊者，將可接手核心 RDBMS 作業。

受影響版本：

Oracle Database Server 12.1.0.2、12.2.0.1 及 18c 版本。

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0
分析分數：7.2（原廠自評）
分析向量：AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

防護方式：

相關資訊請參考

TLP:WHITE

https://www.oracle.com/technetwork/security-advisory/cpujan2019verbose-5072807.html#DB

Oracle 發布了解決此漏洞的軟體更新。

請以 Oracle 註冊帳號登入取得更新程式

https://login.oracle.com/mysso/signon.jsp

項次二、CVE-2019-2444

概述：

Oracle Database Server 的核心 RDBMS(Relational Database Management System)元件存在漏洞。

低權限的攻擊者可輕易利用此漏洞，自本地登入至運行核心 RDBMS 之架構中，並入侵核心 RDBMS。

成功的攻擊要求攻擊者與第三人互動且核心 RDBMS 須存在漏洞，攻擊可能對其他產品產生顯著影響。成功利用此漏洞之攻擊者將可接手核心 RDBMS 作業。

受影響版本：

Oracle Database Server 12.2.0.1 及 18c 版本。

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：8.2（原廠自評）

分析向量：AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

防護方式：

TLP:WHITE

相關資訊請參考

https://www.oracle.com/technetwork/security-advisory/cpujan2019verbose-5072807.html#DB

Oracle 發布了解決此漏洞的軟體更新。

請以 Oracle 註冊帳號登入取得更新程式

https://login.oracle.com/mysso/signon.jsp

項次三、CVE-2019-2414

概述：

Oracle Fusion Middleware 的 Oracle HTTP Server 組件（子組件：Web Listener）中存在漏洞。
低權限的攻擊者可輕易利用此漏洞，登入運行 Oracle HTTP Server 的架構並入侵 Oracle HTTP Server，入侵成功將可接管 Oracle HTTP Server。

受影響版本：

Oracle Fusion Middleware 12.2.1.3 版本。

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0
分析分數：7.8（原廠自評）
分析向量：AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

防護方式：

TLP:WHITE

相關資訊請參考

https://www.oracle.com/technetwork/security-advisory/cpujan2019verbose-5072807.html#DB

Oracle 發布了解決此漏洞的軟體更新。

請以 Oracle 註冊帳號登入取得更新程式

https://login.oracle.com/mysso/signon.jsp

項次四、CVE-2019-2435

概述：

Oracle MySQL 資料庫的 MySQL Connectors 組件（子組件：Connector/Python）中存在漏洞。

未經驗證的攻擊者得利用此漏洞，藉由網路 TLS 連線存取以入侵 MySQL Connectors，攻擊者須與第三人互動方能攻擊成功。成功利用此漏洞之攻擊，未經授權即可建立、刪除或修改重要資料的存取權限，或是所有 MySQL Connectors 都無法存取重要資料，或是得以存取所有 MySQL Connector 可存取的資料。

受影響版本：

Oracle MySQL 8.0.13 及之前版本，2.1.8 及之前版本。

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：8.1（原廠自評）

分析向量：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

TLP:WHITE

防護方式：

相關資訊請參考

https://www.oracle.com/technetwork/security-advisory/cpujan2019verbose-5072807.html#DB

Oracle 發布了解決此漏洞的軟體更新。

請以 Oracle 註冊帳號登入取得更新程式

https://login.oracle.com/mysso/signon.jsp

項次五、CVE-2019-2534

概述：

Oracle MySQL 資料庫的 MySQL Server 組件（子組件：Replication）中存在漏洞。

低權限的攻擊者得利用此漏洞，藉由多種網路連線協定入侵 MySQL Server。成功利用此漏洞之攻擊，未經授權即可存取重要資料，或是存取 MySQL Server 所有資料，例如未經授權更新、新增或刪除部分 MySQL Server 可存取的資料。

受影響版本：

Oracle MySQL5.6.42 及之前版本，5.7.24 及之前版本，8.0.13 及之前版本。

影響程度：高

CVSS 向量：

使用版本：CVSS 3.0

分析分數：7.1（原廠自評）

TLP:WHITE

分析向量：AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

防護方式：

相關資訊請參考

https://www.oracle.com/technetwork/security-advisory/cpujan2019verbose-5072807.html#DB

Oracle 發布了解決此漏洞的軟體更新。

請以 Oracle 註冊帳號登入取得更新程式

https://login.oracle.com/mysso/signon.jsp

參考連結：

1. Oracle

https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html