教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026060102061919	發佈時間	2026-06-01 14:16:19
事故類型	ANA-漏洞預警	發現時間	2026-06-01 14:16:19
影響等級	低		

[主旨說明:]【漏洞預警】Oracle 針對旗下多款產品發布重大資安公告

[內容說明:]

轉發　台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202605-00000016

【CVE-2026-46833，CVSS：9.0】 此漏洞存在於 Oracle Database Server 的 Net Service 元件，允許未經身分驗證的攻擊者透過 TLS 存取 Net Service 元件，可能對其他產品造成重大影響。

【CVE-2026-46840，CVSS：10.0】 此漏洞存在於 Oracle REST Data Services 的 Backend-as-a-Service 元件，允許未經身分驗證的攻擊者透過 HTTPS 網路存取 Oracle REST Data Services。

【CVE-2026-46775，CVSS：9.9、CVE-2026-46839，CVSS：9.9】 此漏洞存在於 Oracle REST Data Services 的 Core 元件，低權限的攻擊者可透過 HTTPS 網路存取 Oracle REST Data Services，若成功利用可能導致 Oracle REST Data Services 被完全控制。

【CVE-2026-2332，CVSS：9.1】 此漏洞存在於 Oracle REST Data Services 的 Core (Eclipse Jetty)元件，允許未經身分驗證的攻擊者透過 HTTPS 網路存取 Oracle REST Data Services，若成功利用可能導致未經授權新增、刪除或修改關鍵數據。

【CVE-2026-33557，CVSS：9.1】 此漏洞存在於 Oracle Communications

Unified Assurance 的 Message Bus (Apache Kafka)元件，允許未經身分驗證的攻擊者透過 TCP 網路存取 Oracle Communications Unified Assurance，若成功利用可能導致未經授權新增、刪除或修改關鍵數據。

【CVE-2025-15467，CVSS：8.8】 此漏洞存在於 Oracle Communications Unified Assurance 的 Core (MySQL Server)元件，允許未經身分驗證的攻擊者透過 HTTP 網路存取 Oracle Communications Unified Assurance。若要成功利用此漏洞需仰賴除攻擊者之外的其他使用者互動。

【CVE-2026-41044，CVSS：8.8】 此漏洞存在於 Oracle Communications Unified Assurance 的 Message Bus (Apache Kafka)元件，低權限的攻擊者可透過 HTTPS 網路存取 Oracle Communications Unified Assurance，若成功利用可能導致 Oracle Communications Unified Assurance 被完全控制。

【CVE-2026-46822，CVSS：9.9】 此漏洞存在於 Oracle iAssets 的 Internal Operations 元件，低權限的攻擊者可透過 HTTPS 網路存取 Oracle iAssets 並使其遭受攻擊，若成功利用可能導致 Oracle iAssets 被完全控制。

【CVE-2026-46824，CVSS：9.9】 此漏洞存在於 Oracle Universal Work Queue 的 Work Provider Site Level Administration 元件，低權限的攻擊者可透過 HTTPS 網路存取 Oracle Universal Work Queue，若成功利用可能導致 Oracle Universal Work Queue 被完全控制。

【CVE-2026-46817，CVSS：9.8】 此漏洞存在於 Oracle Payments 的 File Transmission 元件，允許未經身分驗證的攻擊者透過 HTTP 網路存取 Oracle Payments，若成功利用可能導致 Oracle Payments 被完全控制。

【CVE-2026-46819，CVSS：9.1】 此漏洞存在於 Oracle Internet Procurement Connector 的 Internal Operations 元件，允許未經身分驗證的攻擊者透過 HTTP 網路存取 Oracle Internet Procurement Connector，若成功利用可能導致未經授權新增、刪除或修改關鍵數據。

【CVE-2026-46837，CVSS：8.8】 此漏洞存在於 Oracle Flow Manufacturing 的 Security 元件，低權限的攻擊者可透過 SQL 存取網路，若成功利用可能導致 Oracle Flow Manufacturing 被完全控制。

【CVE-2026-46826，CVSS：8.8】 此漏洞存在於 Oracle Payroll 的 Internal Operations 元件，低權限的攻擊者可透過 HTTPS 網路存取，若成功利用可能

導致 Oracle Payroll 被完全控制。

【CVE-2026-46827，CVSS：8.8】 此漏洞存在於 Oracle Payroll 的 Self Service Manager 元件，低權限的攻擊者可透過 HTTP 網路存取，若成功利用可能導致 Oracle Payroll 被完全控制。

【CVE-2026-34311，CVSS：9.8】 此漏洞存在於 Oracle Hospitality OPERA 5 Property Services 的 Opera 元件，允許未經身分驗證的攻擊者透過 HTTP 網路存取 Oracle Hospitality OPERA 5 Property Services，若成功利用可能導致 OPERA 5 Property Services 被完全控制。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

Oracle Communications Unified Assurance 6.11 至 7.00 版本

Oracle Database Server 23.4.0 至 23.26.2 版本

Oracle Flow Manufacturing 12.2.3 至 12.2.15 版本

Oracle Hospitality OPERA 5 Property Services 5.6.19.24

Oracle Hospitality OPERA 5 Property Services 5.6.22

Oracle Hospitality OPERA 5 Property Services 5.6.25.19

Oracle Hospitality OPERA 5 Property Services 5.6.27.6

Oracle Hospitality OPERA 5 Property Services 5.6.28

Oracle iAssets 12.2.3 至 12.2.15 版本

Oracle Internet Procurement Connector 12.2.3 至 12.2.15 版本

Oracle Payments 12.2.3 至 12.2.15 版本

Oracle Payroll 12.2.3 至 12.2.15 版本 Oracle REST Data Services 24.2.0 至 26.1.0 版本 Oracle Universal Work Queue 12.2.3 至 12.2.15 版本
[建議措施:] 根據官方網站釋出的解決方式進行修補: https://www.oracle.com/security-alerts/cspumay2026.html
[參考資料:] 1. https://www.twcert.org.tw/tw/cp-169-10945-d47ee-1.html