國立成功大學 National Cheng Kung University

ANA事件單通知:TACERT-ANA-2026060102061919【漏洞預警】Oracle針對旗下多款產品發布重大資安公告

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

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw