Post Date: 2026/06/04

Vulnerability Alert Oracle Releases Critical Security Advisory for Multiple Products

- Subject: Vulnerability Alert Oracle Releases Critical Security Advisory for Multiple Products

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center Security Advisory TWCERTCC-200-202605-00000016
  - CVE-2026-46833, CVSS: 9.0 This vulnerability exists in the Net Service component of Oracle Database Server, allowing unauthenticated attackers to access the Net Service component via TLS, which may significantly impact other products.
  - CVE-2026-46840, CVSS: 10.0 This vulnerability exists in the Backend-as-a-Service component of Oracle REST Data Services, allowing unauthenticated attackers to access Oracle REST Data Services via an HTTPS network.
  - CVE-2026-46775, CVSS: 9.9; CVE-2026-46839, CVSS: 9.9 This vulnerability exists in the Core component of Oracle REST Data Services, allowing low-privileged attackers to access Oracle REST Data Services via an HTTPS network. Successful exploitation could lead to complete control over Oracle REST Data Services.
  - CVE-2026-2332, CVSS: 9.1 This vulnerability exists in the Core (Eclipse Jetty) component of Oracle REST Data Services, allowing unauthenticated attackers to access Oracle REST Data Services via an HTTPS network. Successful exploitation could result in unauthorized creation, deletion, or modification of critical data.
  - CVE-2026-33557, CVSS: 9.1 This vulnerability exists in the Message Bus (Apache Kafka) component of Oracle Communications Unified Assurance, allowing unauthenticated attackers to access Oracle Communications Unified Assurance via a TCP network. Successful exploitation could result in unauthorized creation, deletion, or modification of critical data.
  - CVE-2025-15467, CVSS: 8.8 This vulnerability exists in the Core (MySQL Server) component of Oracle Communications Unified Assurance, allowing unauthenticated attackers to access Oracle Communications Unified Assurance via an HTTP network. Successful exploitation relies on interaction from users other than the attacker.
  - CVE-2026-41044, CVSS: 8.8 This vulnerability exists in the Message Bus (Apache Kafka) component of Oracle Communications Unified Assurance, allowing low-privileged attackers to access Oracle Communications Unified Assurance via an HTTPS network. Successful exploitation could lead to complete control over Oracle Communications Unified Assurance.
  - CVE-2026-46822, CVSS: 9.9 This vulnerability exists in the Internal Operations component of Oracle iAssets, allowing low-privileged attackers to access and attack Oracle iAssets via an HTTPS network. Successful exploitation could lead to complete control over Oracle iAssets.
  - CVE-2026-46824, CVSS: 9.9 This vulnerability exists in the Work Provider Site Level Administration component of Oracle Universal Work Queue, allowing low-privileged attackers to access Oracle Universal Work Queue via an HTTPS network. Successful exploitation could lead to complete control over Oracle Universal Work Queue.
  - CVE-2026-46817, CVSS: 9.8 This vulnerability exists in the File Transmission component

of Oracle Payments, allowing unauthenticated attackers to access Oracle Payments via an HTTP network. Successful exploitation could lead to complete control over Oracle Payments.
    - CVE-2026-46819, CVSS: 9.1 This vulnerability exists in the Internal Operations component of Oracle Internet Procurement Connector, allowing unauthenticated attackers to access Oracle Internet Procurement Connector via an HTTP network. Successful exploitation could result in unauthorized creation, deletion, or modification of critical data.
    - CVE-2026-46837, CVSS: 8.8 This vulnerability exists in the Security component of Oracle Flow Manufacturing, allowing low-privileged attackers to gain access via a network utilizing SQL. Successful exploitation could lead to complete control over Oracle Flow Manufacturing.
    - CVE-2026-46826, CVSS: 8.8 This vulnerability exists in the Internal Operations component of Oracle Payroll, allowing low-privileged attackers to gain access via an HTTPS network. Successful exploitation could lead to complete control over Oracle Payroll.
    - CVE-2026-46827, CVSS: 8.8 This vulnerability exists in the Self Service Manager component of Oracle Payroll, allowing low-privileged attackers to gain access via an HTTP network. Successful exploitation could lead to complete control over Oracle Payroll.
    - CVE-2026-34311, CVSS: 9.8 This vulnerability exists in the Opera component of Oracle Hospitality OPERA 5 Property Services, allowing unauthenticated attackers to access Oracle Hospitality OPERA 5 Property Services via an HTTP network. Successful exploitation could lead to complete control over OPERA 5 Property Services.
- Affected Platforms:
    - Oracle Communications Unified Assurance versions 6.11 to 7.00
    - Oracle Database Server versions 23.4.0 to 23.26.2
    - Oracle Flow Manufacturing versions 12.2.3 to 12.2.15
    - 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 versions 12.2.3 to 12.2.15
    - Oracle Internet Procurement Connector versions 12.2.3 to 12.2.15
    - Oracle Payments versions 12.2.3 to 12.2.15
    - Oracle Payroll versions 12.2.3 to 12.2.15
    - Oracle REST Data Services versions 24.2.0 to 26.1.0
    - Oracle Universal Work Queue versions 12.2.3 to 12.2.15
- Recommendations:
    - Apply patches according to the solutions released on the official website: https://www.oracle.com/security-alerts/cspumay2026.html
- References:
    1. https://www.twcert.org.tw/tw/cp-169-10945-d47ee-1.html

---

Computer and Communication Center
Network Systems Division Sincerely

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260604_21

Last update: **2026/06/04 09:33**