مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Oracle April 2026 Critical Patch Update

Tracking #:432318833

Date:23-04-2026



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Oracle Corporation has released its April 2026 Critical Patch Update (CPU), addressing 481 security vulnerabilities across 28 product families.

## TECHNICAL DETAILS:

Oracle Corporation has released its April 2026 Critical Patch Update (CPU), addressing 481 security vulnerabilities across 28 product families. A significant portion of these vulnerabilities are classified as high to critical severity, with many enabling remote code execution (RCE) and unauthenticated network exploitation.

**Detailed Analysis**

**Overall Vulnerability Distribution**

- **Total vulnerabilities patched:** 481
- **Product families affected:** 28
- **Third-party CVEs:** 376 (~78%)
- **Highest impacted products:**
  - Oracle Communications: 139 vulnerabilities
  - Oracle Financial Services Applications: 75 vulnerabilities
  - Oracle Fusion Middleware: 59 vulnerabilities

**Key Affected Platforms**

- Oracle Middleware
- Oracle E-Business Suite
- Oracle Communications
- Oracle Database ecosystem (including:
  - Database Server
  - Autonomous Health Framework
  - GoldenGate
  - REST Data Services
  - TimesTen)

**Critical Vulnerability Highlights**

**Oracle Communications**

- **Total patches:** 139
- **Unauthenticated remote exploits:** 93

**Notable CVEs:**

- CVE-2025-6965 — CVSS 9.8
- CVE-2025-68615 — CVSS 9.6
- CVE-2026-25968 — CVSS 9.8
- CVE-2025-48913 — CVSS 9.1
- CVE-2025-12543 — CVSS 9.8
- CVE-2024-5535 — CVSS 9.1
- CVE-2025-55130 — CVSS 9.8
- CVE-2025-58050 — CVSS 9.1

**Impact:**

- Remote Code Execution (RCE)

- Full system compromise without credentials

**Oracle Financial Services Applications**

- **Total patches:** 75
- **Unauthenticated vulnerabilities:** 59

**Critical CVEs:**

- CVE-2023-34034 — CVSS 9.8
- CVE-2023-44981 — CVSS 9.1

**Impact:**

- Remote Code Execution
- Risk to financial data integrity and transaction systems

**Oracle Fusion Middleware**

- **Total patches:** 59
- **Unauthenticated vulnerabilities:** 46

**Critical CVEs:**

- CVE-2022-45047 — CVSS 9.8
- CVE-2025-68615 — CVSS 9.1
- CVE-2026-34285 — CVSS 9.8
- CVE-2026-34286 — CVSS 9.8
- CVE-2026-34287 — CVSS 9.0
- CVE-2021-45046 — CVSS 9.0

**Impact:**

- RCE via middleware services
- Potential enterprise-wide compromise

**Oracle MySQL**

- **Total patches:** 34
- **Unauthenticated vulnerabilities:** 3

**Critical CVE:**

- CVE-2025-15467 — CVSS 9.8
    - Affects MySQL Enterprise Backup

**Impact:**

- Remote Code Execution
- Backup system compromise leading to data exposure

**Oracle E-Business Suite**

- **Total patches:** 18
- **Unauthenticated vulnerabilities:** 8

**Critical CVE:**

- CVE-2026-34275 — CVSS 9.8
    - Component: Advanced Inbound Telephony

**Impact:**

- RCE in enterprise resource planning (ERP) environments
- Potential access to sensitive business data

**Oracle Database Ecosystem**

- **Total updates:** 27
- Breakdown:
- Database Server: 8 patches (max CVSS 7.5)

- Autonomous Health Framework: 2 patches (CVSS 7.2)
- Blockchain Platform: 3 patches (CVSS 7.5)
- GoldenGate: 10 patches (CVSS 7.5)
- REST Data Services: 2 patches (CVSS 7.5)
- TimesTen: 1 patch (CVSS 7.4)

## RECOMMENDATIONS:

**Immediate Actions**

- Apply April 2026 CPU patches without delay
- Prioritize:
  - Internet-facing systems
  - Oracle Communications and Middleware deployments
  - Financial and ERP systems

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://www.oracle.com/security-alerts/cpuapr2026.html