مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Oracle

Tracking #:432319164

Date:19-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Oracle has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Oracle has released its June 2026 Critical Security Patch Update (CSPU), addressing 245 security vulnerabilities across multiple Oracle product families, including Oracle Fusion Middleware, WebLogic Server, Oracle Enterprise Manager, Oracle E-Business Suite, Oracle MySQL, JD Edwards, PeopleSoft, Oracle Solaris, and Oracle Coherence.

Several vulnerabilities are rated Critical with CVSS scores of up to 10.0 and are remotely exploitable without authentication. Successful exploitation could allow attackers to execute arbitrary code, gain unauthorized access, disclose sensitive information, modify data, or cause complete compromise of affected systems.

Key Vulnerabilities
Critical Severity Vulnerabilities

- **CVE-2026-35308, CVE-2026-35307 – Oracle Coherence**
  Severity: Critical | **CVSS:** 10.0
  Remotely exploitable vulnerabilities that require no authentication and could allow complete compromise of affected systems.
- **CVE-2026-46778, CVE-2026-46781 – Oracle WebCenter Enterprise Capture**
  Severity: Critical | **CVSS:** 10.0
  Unauthenticated remote vulnerabilities that may enable attackers to gain full control of vulnerable instances.
- **CVE-2026-46803, CVE-2026-46846 – Oracle WebCenter Portal**
  Severity: Critical | **CVSS:** 10.0
  Remote vulnerabilities that can be exploited without authentication, potentially resulting in unauthorized access and system compromise.
- **CVE-2026-46798, CVE-2026-46800 – Oracle WebCenter Sites**
  Severity: Critical | **CVSS:** 10.0
  Critical flaws that could allow unauthenticated attackers to compromise affected WebCenter Sites deployments.
- **CVE-2026-35301, CVE-2026-35292 – Oracle WebLogic Server**
  Severity: Critical | **CVSS:** 10.0
  Remotely exploitable vulnerabilities in WebLogic Server that may lead to complete compromise of vulnerable servers.

Additional Critical Vulnerabilities (CVSS 9.8)
Oracle also addressed multiple remotely exploitable vulnerabilities with CVSS scores of **9.8**, affecting:

- Oracle Enterprise Manager Base Platform (CVE-2026-46857)
- Oracle Coherence (CVE-2026-35309, CVE-2026-35310, CVE-2026-35304)
- Oracle Unified Directory (CVE-2026-46773, CVE-2026-46774)
- Oracle Virtual Directory (CVE-2026-35312)
- Oracle WebCenter Content (multiple CVEs)

- Oracle WebCenter Sites (multiple CVEs)
- WebCenter Content: Imaging (CVE-2026-46783)
- WebLogic Server (CVE-2026-35300)
- JD Edwards EnterpriseOne Tools (multiple CVEs)
- MySQL Router (CVE-2026-46860)

Note:
Refer to the Oracle Critical Patch Update Advisory – June 2026 for additional CVEs and detailed information regarding affected products, impacted software versions, fixed releases, and recommended mitigation measures.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Oracle.

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/cspujun2026.html