مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Oracle July 2026 Critical Patch Update

Tracking #:432319329

Date:23-07-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Oracle has released its July 2026 Critical Patch Update (CPU) addressing 1,235 unique CVEs through 1,449 security updates across 32 Oracle product families.

TECHNICAL DETAILS:

Oracle has released its July 2026 Critical Patch Update (CPU) addressing 1,235 unique CVEs through 1,449 security updates across 32 Oracle product families. The update includes 261 Critical patches affecting 228 Critical CVEs.
Among the most significant issues are multiple Critical Remote Code Execution (RCE) vulnerabilities affecting Oracle WebLogic Server. Several vulnerabilities allow unauthenticated remote attackers to compromise vulnerable servers over commonly exposed protocols including T3, IIOP, HTTP, SOAP, and SAML.

Oracle July 2026 CPU Highlights

- **1,449** total security patches released.
- **1,235** unique CVEs addressed.
- **261 Critical** patches covering **228 Critical CVEs**.
- **763 High** severity patches.
- **355** patches affect Oracle Fusion Middleware.
- **219** Fusion Middleware vulnerabilities are remotely exploitable without authentication.

Notable Vulnerability Details

- **CVE-2026-60198 – Java Deserialization Remote Code Execution**
  - **CVSS v3.1:** 9.8 (Critical)
  - Exploitable remotely without authentication.
  - Affects T3/IIOP protocols.
  - May allow complete server compromise.
- **CVE-2026-60202 – Java Deserialization Remote Code Execution**
  - **CVSS v3.1:** 9.8 (Critical)
  - Unauthenticated remote exploitation.
  - Impacts T3/IIOP communication.
  - Enables arbitrary code execution.
- **CVE-2026-60204 – Java Deserialization Remote Code Execution**
  - **CVSS v3.1:** 9.8 (Critical)
  - Exploitable over T3/IIOP.
  - No authentication required.
  - May result in full system takeover.
- **CVE-2026-60199 – HTTP Remote Code Execution**
  - **CVSS v3.1:** 9.8 (Critical)
  - Exploitable remotely via HTTP.
  - Requires no authentication.
  - Can lead to complete server compromise.
- **CVE-2026-60200 – SOAP Remote Code Execution**
  - **CVSS v3.1:** 9.8 (Critical)
  - Exploitable through SOAP endpoints.
  - Unauthenticated attacker can execute arbitrary code remotely.

- **CVE-2026-60206 – SAML Privilege Escalation / Cross-Scope Impact**
  - **CVSS v3.1:** 9.9 (Critical)
  - Exploitable through SAML.
  - Requires low privileges.
  - May impact additional Oracle products by changing security scope.
- **CVE-2026-60208 – HTTP Confidentiality and Integrity Compromise**
  - **CVSS v3.1:** 9.1 (Critical)
  - Exploitable remotely over HTTP.
  - No authentication required.
  - May compromise sensitive data and modify application integrity.
- **CVE-2026-60201 – High Complexity Remote Vulnerability**
  - **CVSS v3.1:** 8.1 (High)
  - Affects T3/IIOP.
  - Exploitable without authentication.
  - Higher attack complexity reduces practical exploitation likelihood.

Affected and fixed versions:

- Refer to the July 2026 advisory for full details.

RECOMMENDATIONS:

Immediate Actions:

- Refer to the Oracle CPU July 2026 advisory and apply all relevant patches.

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/cpujul2026.html