مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Oracle Critical Patch Update – January 2026

Tracking #:432318287

Date:21-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Oracle released its quarterly Critical Patch Update (CPU), addressing a total of 337 new security vulnerabilities across multiple product families.

TECHNICAL DETAILS:

Oracle's Critical Patch Update (CPU) for January 2026 addresses 337 new security patches for vulnerabilities across 30+ product families, including Database, Java SE, Fusion Middleware, MySQL, Communications, E-Business Suite, Financial Services, and others.
Among the fixes are 158 unique CVEs, with critical vulnerabilities (CVSS 9.0-10.0) comprising about 8% of the update, high-severity (7.0-8.9) at 45.7%, and the rest medium to low. Many issues are remotely exploitable without authentication, posing risks of unauthorized access, data manipulation, and denial-of-service.

Notable CVEs:

- **CVE-2026-21962 — Score: 10.0** Affected Products/Versions: Oracle HTTP Server and WebLogic Server Proxy Plug-in (Apache: 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0); WebLogic Server Proxy Plug-in for IIS (12.2.1.4.0 only)
- **CVE-2025-66516 — Score: 10.0** Affected Products/Versions: Commerce Guided Search (11.4.0); Communications Order and Service Management (7.5.0, 8.0.0); Unified Assurance (6.1.0–6.1.1); PeopleSoft Enterprise PeopleTools (8.60–8.62).
- **CVE-2025-49844 — Score: 9.9** Affected Products/Versions: Communications Operations Monitor (5.2).
- **CVE-2021-43113 — Score: 9.8** Affected Products/Versions: Construction and Engineering Primavera Unifier (21.12.0–25.12.0, including specific sub-ranges like 21.12.0–21.12.17, 22.12.0–22.12.15, etc.).
- **CVE-2025-6965 — Score: 9.8** Affected Products/Versions: MySQL Server (8.4.0–8.4.7, Docker images); PeopleSoft Enterprise PeopleTools (8.60–8.62).
- **CVE-2024-52046 — Score: 9.8** Affected Products/Versions: Healthcare Health Sciences Information Manager (4.0.0).
- **CVE-2026-21969 — Score: 9.8** Affected Products/Versions: Supply Chain Agile PLM for Process (6.2.4).
- **CVE-2025-54874 — Score: 9.8** Affected Products/Versions: Supply Chain AutoVue Office (21.1.0; also applies to related 2D/3D/EDA/Electro-Mechanical variants).
- **CVE-2025-49796 — Score: 9.1** Affected Products/Versions: Financial Services Banking Branch (14.5.0–14.8.0), Cash Management (14.8.1), Corporate Lending Process Management (14.5.0–14.7.0), Liquidity Management (14.8.1), Supply Chain Finance (14.8.1); also impacts related components in Oracle HTTP Server (12.2.1.4.0, 14.1.2.0.0) and Hyperion Infrastructure Technology (11.2.23).
- **CVE-2026-21945**- Server-Side Request Forgery (SSRF) in Oracle Java a that is remotely exploitable without authentication. Affected Products/Versions:Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17, 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16

RECOMMENDATIONS:

- Immediate Patching: Apply the January 2026 CPU patches promptly for all affected supported

versions.

- Prioritize Patch Application: Apply CPU patches immediately for high and critical severity vulnerabilities, especially for systems with external network exposure or high business impact.

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/cpujan2026.html