# Oracle Critical Patch Update April 2026: Waratek Coverage Report

2026-Q2 · Rulepack `vcpu-rulepack-2026-06-18-b106`

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

## Coverage Summary

| 241 | 105 | 105 | 3 |
|---|---|---|---|
| CVEs in CPU | In scope for Java | Categorized | ARMR patches |

### By coverage mechanism

| | |
|---|---|
| ARMR patch | 3 |
| ARMR secure-rule | 5 |
| Other mitigation | 1 |
| No exploit disclosure | 35 |
| Patch feasible | 61 |
| Out of scope | 136 |

### By severity

| | |
|---|---|
| CRITICAL | 18 |
| HIGH | 93 |
| MEDIUM | 117 |
| LOW | 13 |

## Affected Oracle Product Families

Shows where in your Oracle stack this CPU lands. Use this to decide whether the rulepack matters for you.

| PRODUCT FAMILY | COVERAGE | AFFECTED VERSIONS |
|---|---|---|
| Oracle Communications<br>65 CVEs in this CPU | 23 / 23 covered | · 15.0<br>· 15.0.0.0–15.0.1.0, 15.1.0.0–15.2.0.0<br>· 15.0.0.0.0<br>+23 more |
| Oracle Fusion Middleware<br>46 CVEs in this CPU | 34 / 34 covered | · 12.2.1.4.0<br>· 12.2.1.4.0, 12.1.3.0.0<br>· 12.2.1.4.0, 14.1.1.0.0<br>+14 more |
| Oracle Financial Services Applications<br>33 CVEs in this CPU | 28 / 28 covered | · 1.0.2.1<br>· 12.2.3–12.2.15<br>· 14.5.0.0.0–14.8.0.0.0<br>+13 more |
| Oracle MySQL<br>31 CVEs in this CPU | 0 / 0 covered | · 25.1.200<br>· 25.1.204<br>· 8.0.0–8.0.45<br>+3 more |
| Oracle PeopleSoft<br>21 CVEs in this CPU | 5 / 5 covered | · 15.0<br>· 25.1.200<br>· 25.1.204<br>+4 more |
| Oracle Analytics<br>15 CVEs in this CPU | 10 / 10 covered | · 12.2.3–12.2.15<br>· 15.0<br>· 7.6.0.0.0, 8.2.0.0.0<br>+1 more |
| Oracle E-Business Suite<br>13 CVEs in this CPU | 7 / 7 covered | · 12.2.3–12.2.15<br>· 12.2.7–12.2.15<br>· 12.2.9–12.2.15<br>+1 more |
| Oracle Siebel CRM<br>13 CVEs in this CPU | 10 / 10 covered | · 14.5.0.0.0–14.8.0.0.0<br>· 15.0<br>· 17.0–25.11<br>+5 more |
| Oracle Java SE<br>11 CVEs in this CPU | 6 / 6 covered | · Oracle Java SE: 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18, 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17<br>· Oracle Java SE: 25.0.1<br>· Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle |

| PRODUCT FAMILY | COVERAGE | AFFECTED VERSIONS |
| --- | --- | --- |
| | | GraalVM for JDK: 17.0.18, 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17<br>+3 more |
| Oracle GoldenGate<br>9 CVEs in this CPU | 8 / 8 covered | · 14.1.2.0.0<br>· 14.8.1.0.0<br>· 15.0<br>+4 more |
| Oracle Virtualization<br>9 CVEs in this CPU | 0 / 0 covered | · 7.2.6 |
| Oracle Database Server<br>8 CVEs in this CPU | 3 / 3 covered | · 19.3–19.30<br>· 19.3–19.30, 21.3–21.21<br>· 19.3–19.30, 21.3–21.21, 23.4.0–23.26.1<br>+4 more |
| Oracle Enterprise Manager<br>6 CVEs in this CPU | 4 / 4 covered | · 11.4.0<br>· 12.2.1.4.0<br>· 13.5, 24.1<br>+3 more |
| Oracle Hyperion<br>6 CVEs in this CPU | 3 / 3 covered | · 11.2.24.0.000<br>· 15.0.0.0–15.0.1.0, 15.1.0.0–15.2.0.0<br>· 6.1.1–7.0.0 |
| Oracle Utilities Applications<br>6 CVEs in this CPU | 4 / 4 covered | · 15.0<br>· 23.1.5–23.3.0<br>· 25.1.204<br>+3 more |
| Oracle Construction and Engineering<br>4 CVEs in this CPU | 3 / 3 covered | · 12.2.1.4.0<br>· 15.0<br>· 25.1.200<br>+1 more |
| Oracle Life Science Applications<br>4 CVEs in this CPU | 1 / 1 covered | · 15.0<br>· 7.0.1.0, 7.0.1.1<br>· 9.2.1–9.2.3 |
| Oracle Supply Chain<br>4 CVEs in this CPU | 1 / 1 covered | · 15.0<br>· 21.1.0<br>· 25.1.204<br>+1 more |
| Oracle Blockchain Platform<br>3 CVEs in this CPU | 0 / 0 covered | · 24.1.3<br>· 25.1.204 |
| Oracle Commerce<br>3 CVEs in this CPU | 2 / 2 covered | · 11.4.0<br>· 12.2.3–12.2.15<br>· 23.1.5–23.3.0 |

| PRODUCT FAMILY | COVERAGE | AFFECTED VERSIONS |
| --- | --- | --- |
| Oracle JD Edwards<br>3 CVEs in this CPU | 1 / 1 covered | · 6.1.1–7.0.0<br>· 7.6.0.0.0, 8.2.0.0.0<br>· 9.2.0.0–9.2.26.1 |
| Oracle Retail Applications<br>3 CVEs in this CPU | 3 / 3 covered | · 15.0<br>· 21.0.5, 22.0.3<br>· 7.6.0.0.0, 8.2.0.0.0 |
| Oracle Adapter for Eclipse RDF4J<br>2 CVEs in this CPU | 2 / 2 covered | · 24.1.0<br>· 24.2.1 |
| Oracle Autonomous Health Framework<br>2 CVEs in this CPU | 0 / 0 covered | · 25.11–26.1<br>· 8.2.0.0.0 |
| Oracle REST Data Services<br>2 CVEs in this CPU | 2 / 2 covered | · 24.2.0, 24.2.1, 24.3.0, 24.3.1, 24.4.0, 25.1.1, 25.2.0, 25.2.1, 25.2.2, 25.2.3, 25.3.0, 25.3.1, 25.4.0<br>· 25.1.201, 25.2.100 |
| Oracle Systems<br>2 CVEs in this CPU | 0 / 0 covered | · 11.4<br>· 8.8 |
| Oracle Hospitality Applications<br>1 CVE in this CPU | 1 / 1 covered | · 23.1.5–23.3.0 |
| Oracle TimesTen In-Memory Database<br>1 CVE in this CPU | 0 / 0 covered | · 18.1.4, 22.1.1 |

## Changes Since Prior CPU

Comparing against **Oracle Critical Patch Update January 2026** (rulepack `vcpu-rulepack-2026-06-04-b85`)

### 197 new CVEs in this CPU advisory

| | | | |
|---|---|---|---|
| CVE-2026-35252 | CVE-2026-34307 | CVE-2026-34269 | CVE-2026-22003 |
| CVE-2026-35251 | CVE-2026-34306 | CVE-2026-34268 | CVE-2026-22002 |
| CVE-2026-35250 | CVE-2026-34305 | CVE-2026-34267 | CVE-2026-22001 |
| CVE-2026-35249 | CVE-2026-34304 | CVE-2026-34266 | CVE-2026-21999 |
| CVE-2026-35248 | CVE-2026-34303 | CVE-2026-33870 | CVE-2026-21998 |
| CVE-2026-35247 | CVE-2026-34302 | CVE-2026-3288 | CVE-2026-21997 |
| CVE-2026-35246 | CVE-2026-34301 | CVE-2026-31790 | CVE-2026-21637 |
| CVE-2026-35245 | CVE-2026-34300 | CVE-2026-27830 | CVE-2026-21452 |
| CVE-2026-35244 | CVE-2026-34299 | CVE-2026-27727 | CVE-2026-21441 |
| CVE-2026-35243 | CVE-2026-34298 | CVE-2026-27099 | CVE-2026-20652 |
| CVE-2026-35242 | CVE-2026-34297 | CVE-2026-26007 | CVE-2026-1642 |
| CVE-2026-35241 | CVE-2026-34296 | CVE-2026-25990 | CVE-2026-0861 |
| CVE-2026-35240 | CVE-2026-34295 | CVE-2026-25968 | CVE-2025-9232 |
| CVE-2026-35239 | CVE-2026-34294 | CVE-2026-25646 | CVE-2025-8869 |
| CVE-2026-35238 | CVE-2026-34293 | CVE-2026-25210 | CVE-2025-69223 |
| CVE-2026-35237 | CVE-2026-34292 | CVE-2026-24734 | CVE-2025-68973 |
| CVE-2026-35236 | CVE-2026-34291 | CVE-2026-23903 | CVE-2025-68615 |
| CVE-2026-35235 | CVE-2026-34290 | CVE-2026-23865 | CVE-2025-68431 |
| CVE-2026-35234 | CVE-2026-34289 | CVE-2026-23490 | CVE-2025-68121 |
| CVE-2026-35232 | CVE-2026-34288 | CVE-2026-22801 | CVE-2025-67635 |
| CVE-2026-35231 | CVE-2026-34287 | CVE-2026-22184 | CVE-2025-66453 |
| CVE-2026-35230 | CVE-2026-34286 | CVE-2026-22022 | CVE-2025-64775 |
| CVE-2026-35229 | CVE-2026-34285 | CVE-2026-22021 | CVE-2025-61984 |
| CVE-2026-34325 | CVE-2026-34284 | CVE-2026-22019 | CVE-2025-61729 |
| CVE-2026-34324 | CVE-2026-34283 | CVE-2026-22018 | CVE-2025-59775 |
| CVE-2026-34323 | CVE-2026-34282 | CVE-2026-22017 | CVE-2025-59465 |
| CVE-2026-34321 | CVE-2026-34281 | CVE-2026-22016 | CVE-2025-58754 |
| CVE-2026-34320 | CVE-2026-34280 | CVE-2026-22015 | CVE-2025-58181 |
| CVE-2026-34319 | CVE-2026-34279 | CVE-2026-22014 | CVE-2025-58050 |
| CVE-2026-34318 | CVE-2026-34278 | CVE-2026-22013 | CVE-2025-55754 |
| CVE-2026-34317 | CVE-2026-34277 | CVE-2026-22011 | CVE-2025-55130 |
| CVE-2026-34315 | CVE-2026-34276 | CVE-2026-22010 | CVE-2025-52967 |
| CVE-2026-34314 | CVE-2026-34275 | CVE-2026-22009 | CVE-2025-48913 |
| CVE-2026-34313 | CVE-2026-34274 | CVE-2026-22008 | CVE-2025-46762 |
| CVE-2026-34312 | CVE-2026-34273 | CVE-2026-22007 | CVE-2025-46392 |
| CVE-2026-34310 | CVE-2026-34272 | CVE-2026-22006 | CVE-2025-41254 |
| CVE-2026-34309 | CVE-2026-34271 | CVE-2026-22005 | CVE-2025-41253 |
| CVE-2026-34308 | CVE-2026-34270 | CVE-2026-22004 | CVE-2025-41242 |

| | | | |
|---|---|---|---|
| CVE-2025-35036 | CVE-2025-13601 | CVE-2024-36124 | CVE-2023-26464 |
| CVE-2025-33042 | CVE-2025-13151 | CVE-2024-31573 | CVE-2023-20863 |
| CVE-2025-31948 | CVE-2025-12543 | CVE-2024-29857 | CVE-2023-1436 |
| CVE-2025-27821 | CVE-2025-11143 | CVE-2024-29371 | CVE-2022-45688 |
| CVE-2025-27820 | CVE-2025-0725 | CVE-2023-5388 | CVE-2021-45046 |
| CVE-2025-27636 | CVE-2024-8184 | CVE-2023-52428 | CVE-2021-28168 |
| CVE-2025-24970 | CVE-2024-7254 | CVE-2023-46750 | CVE-2021-22573 |
| CVE-2025-1948 | CVE-2024-6387 | CVE-2023-44981 | CVE-2021-0341 |
| CVE-2025-15467 | CVE-2024-5535 | CVE-2023-35116 | CVE-2020-17521 |
| CVE-2025-15284 | CVE-2024-51504 | CVE-2023-34453 | |
| CVE-2025-14104 | CVE-2024-45339 | CVE-2023-34034 | |
| CVE-2025-14017 | CVE-2024-43394 | CVE-2023-2976 | |

### 1 CVEs newly covered by this rulepack

ARMR patches added since prior rulepack that address CVEs in this CPU.

CVE-2026-22016

### 4 rulepacks changed in this release

Replace only these `{year}vcpu.armr` files in your VCPU pack — rulepacks not listed here are unchanged since the prior release.

#### 2026vcpu.armr

ADDED CVE-2026-22016

#### 2024vcpu.armr

MODIFIED CVE-2024-21085

#### 2023vcpu.armr

MODIFIED CVE-2023-22067 CVE-2023-21930

#### 2022vcpu.armr

MODIFIED CVE-2022-21294

## Per-CVE Coverage

### CVE-2025-48913 CRITICAL CVSS 9.8 PATCH-FEASIBLE

If untrusted users are allowed to configure JMS for Apache CXF, previously they could use RMI or LDAP URLs, potentially leading to code execution capabilities. This interface is now restricted to reject those protocols, removing this possibility. Users are recommended to upgrade to versions 3.6.8, 4.0.9 or 4.1.3, which fix this issue.

**Product:** Oracle Communications **Component:** Core (Apache CXF) **Affected:** 6.1.1-7.0.0

CWE-20

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.cxf:cxf-rt-transports-jms). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

### CVE-2022-45047 CRITICAL CVSS 9.8 MITIGATED-BY-SECURE-RULE

Class org.apache.sshd.server.keyprovider.SimpleGeneratorHostKeyProvider in Apache MINA SSHD <= 2.9.1 uses Java deserialization to load a serialized java.security.PrivateKey. The class is one of several implementations that an implementor using Apache MINA SSHD can choose for loading the host keys of an SSH server.

**Product:** Oracle Fusion Middleware **Component:** Runtime Server (Apache Mina SSHD) **Affected:** 12.2.1.4.0

CWE-502

**Why this status:** `secure-rule-match` Promoted to MITIGATED-BY-SECURE-RULE: this CVE's weakness (CWE-502: Deserialization of Untrusted Data) can be mitigated by an ARMR deserialization security rule that blocks this class of attack at the JVM level, without requiring a CVE-specific patch.

---

### CVE-2025-12543 CRITICAL CVSS 9.6 PATCH-FEASIBLE

A flaw was found in the Undertow HTTP server core, which is used in WildFly, JBoss EAP, and other Java applications. The Undertow library fails to properly validate the Host header in incoming HTTP requests.As a result, requests containing malformed or malicious Host headers are processed without rejection, enabling attackers to poison caches, perform internal network scans, or hijack user sessions.

**Product:** Oracle Communications **Component:** Alarms, KPI, and Measurements (Undertow) **Affected:** 25.1.200

CWE-20

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: Red Hat published an advisory () confirming a fix exists; the linked Bugzilla ticket (https://bugzilla.redhat.com/show_bug.cgi?id=2408784) traces to the upstream OpenJDK source patch ARMR can derive a rule from.

## CVE-2025-12383 CRITICAL CVSS 9.4 PATCH-FEASIBLE

In Eclipse Jersey versions 2.45, 3.0.16, 3.1.9 a race condition can cause ignoring of critical SSL configurations - such as mutual authentication, custom key/trust stores, and other security settings. This issue may result in SSLHandshakeException under normal circumstances, but under certain conditions, it could lead to unauthorized trust in insecure servers (see PoC)

**Product:** Oracle Communications, Oracle Fusion Middleware **Component:** Configuration (Eclipse Jersey)

**Affected:** 25.1.200

CWE-362

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.glassfish.jersey.core:jersey-client). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2026-34287 CRITICAL CVSS 9.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager...

**Product:** Oracle Fusion Middleware **Component:** Core **Affected:** 12.2.1.4.0

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34286 CRITICAL CVSS 9.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager...

**Product:** Oracle Fusion Middleware **Component:** Core **Affected:** 12.2.1.4.0

CWE-306

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

### CVE-2026-34285 CRITICAL CVSS 9.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager...

**Product:** Oracle Fusion Middleware **Component:** Core **Affected:** 12.2.1.4.0

CWE-306

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

---

### CVE-2026-34279 CRITICAL CVSS 9.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Event Management). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base...

**Product:** Oracle Enterprise Manager **Component:** Event Management **Affected:** 13.5, 24.1

CWE-306

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

---

### CVE-2024-51504 CRITICAL CVSS 9.1 PATCH-FEASIBLE

When using IPAuthenticationProvider in ZooKeeper Admin Server there is a possibility of Authentication Bypass by Spoofing -- this only impacts IP based authentication implemented in ZooKeeper Admin Server. Default configuration of client's IP address detection in IPAuthenticationProvider, which uses HTTP request headers, is weak and allows an attacker to bypass authentication via spoofing client's IP address in request headers. Default configuration honors X-Forwarded-For HTTP header to read client's IP address. X-Forwarded-For request header is mainly used by proxy servers to identify the...

**Product:** Oracle E-Business Suite **Component:** Core (Apache ZooKeeper) **Affected:** 15.0

CWE-290

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.zookeeper:zookeeper). OSV.dev confirms the advisory and the source is publicly available, so a patch may be feasible — this has not been confirmed and requires reviewing the diff between the affected and fixed versions.

## CVE-2023-44981 CRITICAL CVSS 9.1 PATCH-FEASIBLE

Authorization Bypass Through User-Controlled Key vulnerability in Apache ZooKeeper. If SASL Quorum Peer authentication is enabled in ZooKeeper (quorum.auth.enableSasl=true), the authorization is done by verifying that the instance part in SASL authentication ID is listed in zoo.cfg server list. The instance part in SASL auth ID is optional and if it's missing, like 'eve@EXAMPLE.COM', the authorization check will be skipped. As a result an arbitrary endpoint could join the cluster and begin propagating counterfeit changes to the leader, essentially giving it complete read-write access to the...

**Product:** Oracle Financial Services Applications **Component:** Base (Apache ZooKeeper)

**Affected:** 14.5.0.0.0-14.8.0.0.0

CWE-639

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.zookeeper:zookeeper). OSV.dev confirms the advisory and the source is publicly available, so a patch may be feasible — this has not been confirmed and requires reviewing the diff between the affected and fixed versions.

---

## CVE-2023-34034 CRITICAL CVSS 9.1 PATCH-FEASIBLE

Using "**" as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass.

**Product:** Oracle Financial Services Applications **Component:** Onboarding Batch Processes (Spring Security)

**Affected:** 14.5.0.0.0-14.8.0.0.0

CWE-281 CWE-284

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.springframework.security:spring-security-config). OSV.dev confirms the advisory and the source is publicly available, so a patch may be feasible — this has not been confirmed and requires reviewing the diff between the affected and fixed versions.

---

## CVE-2021-45046 CRITICAL CVSS 9.0 MITIGATED-BY-PATCH-RULE

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and...

**Product:** Oracle Fusion Middleware **Component:** Centralized Thirdparty Jars (Apache Log4j)

**Affected:** 12.2.1.4.0

CWE-917 CWE-502

**Why this status:** `ARMR patch` CVE has an ARMR patch rule that provides mitigation

**ARMR:** CVE-2021-45046.armr (https://github.com/waratek/java-patches/blob/develop/rules/libraries/apache/log4j/CVE-2021-45046/patch/2.6/CVE-2021-45046.armr) (spec 2.6)

### CVE-2025-48734 HIGH CVSS 8.8 PATCH-FEASIBLE

Improper Access Control vulnerability in Apache Commons. A special BeanIntrospector class was added in version 1.9.2. This can be used to stop attackers from using the declared class property of Java enum objects to get access to the classloader. However this protection was not enabled by default. PropertyUtilsBean (and consequently BeanUtilsBean) now disallows declared class level property access by default. Releases 1.11.0 and 2.0.0-M2 address a potential security issue when accessing enum properties in an uncontrolled way. If an application using Commons BeanUtils passes property...

**Product:** Oracle E-Business Suite, Oracle Analytics, Oracle Commerce, Oracle Financial Services Applications

**Component:** User Interface (Apache Commons BeanUtils) **Affected:** 12.2.3-12.2.15

CWE-284

---

### CVE-2025-12183 HIGH CVSS 8.8 PATCH-FEASIBLE

Out-of-bounds memory operations in org.lz4:lz4-java 1.8.0 and earlier allow remote attackers to cause denial of service and read adjacent memory via untrusted compressed input.

**Product:** Oracle Financial Services Applications **Component:** Infrastructure (lz4-java) **Affected:** 14.8.0.0.0

CWE-125

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: at.yawk.lz4:lz4-java, org.lz4:lz4-java, org.lz4:lz4-pure-java, net.jpountz.lz4:lz4). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

### CVE-2025-52999 HIGH CVSS 8.7 PATCH-FEASIBLE

jackson-core contains core low-level incremental ("streaming") parser and generator abstractions used by Jackson Data Processor. In versions prior to 2.15.0, if a user parses an input file and it has deeply nested data, Jackson could end up throwing a StackoverflowError if the depth is particularly large. jackson-core 2.15.0 contains a configurable limit for how deep Jackson will traverse in an input document, defaulting to an allowable depth of 1000. jackson-core will throw a StreamConstraintsException if the limit is reached. jackson-databind also benefits from this change because it uses...

**Product:** Oracle Fusion Middleware, Oracle Construction and Engineering, Oracle Enterprise Manager

**Component:** Document Service (jackson-core) **Affected:** 12.2.1.4.0

CWE-121

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (pr tier): https://github.com/FasterXML/jackson-core/pull/943. ARMR can derive a patch from the linked commit.

---

### CVE-2024-7254 HIGH CVSS 8.7 PATCH-FEASIBLE

Any project that parses untrusted Protocol Buffers data containing an arbitrary number of nested groups / series of SGROUP tags can corrupted by exceeding the stack limit i.e. StackOverflow. Parsing nested groups as unknown fields with DiscardUnknownFieldsParser or Java Protobuf Lite parser, or against Protobuf map fields, creates unbounded recursions that can be abused by an attacker.

**Product:** Oracle GoldenGate **Component:** Third Party (Google Protobuf-Java) **Affected:** 23.4-23.10

CWE-400 CWE-674 CWE-787 CWE-20

## CVE-2021-22573 HIGH CVSS 8.7 PATCH-FEASIBLE

The vulnerability is that IDToken verifier does not verify if token is properly signed. Signature verification makes sure that the token's payload comes from valid provider, not from someone else. An attacker can provide a compromised token with custom payload. The token will pass the validation on the client side. We recommend upgrading to version 1.33.3 or above

**Product:** Oracle Fusion Middleware **Component:** Third Party (Google OAuth Client)

**Affected:** 12.2.1.4.0, 14.1.2.0.0

CWE-347

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (pr tier): https://github.com/googleapis/google-oauth-java-client/pull/872. A patch may be feasible — this has not been confirmed and requires reviewing the linked change.

## CVE-2026-22022 HIGH CVSS 8.2 PATCH-FEASIBLE

Deployments of Apache Solr 5.3.0 through 9.10.0 that rely on Solr's "Rule Based Authorization Plugin" are vulnerable to allowing unauthorized access to certain Solr APIs, due to insufficiently strict input validation in those components.  Only deployments that meet all of the following criteria are impacted by this vulnerability: * Use of Solr's "RuleBasedAuthorizationPlugin" * A RuleBasedAuthorizationPlugin config (see security.json) that specifies multiple "roles" * A RuleBasedAuthorizationPlugin permission list (see security.json) that uses one or more of the following...

**Product:** Oracle Communications **Component:** Core (Apache Solr) **Affected:** 6.1.1-7.0.0

CWE-285

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.solr:solr-core). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2025-66566 HIGH CVSS 8.2 PATCH-FEASIBLE

yawkat LZ4 Java provides LZ4 compression for Java. Insufficient clearing of the output buffer in Java-based decompressor implementations in lz4-java 1.10.0 and earlier allows remote attackers to read previous buffer contents via crafted compressed input. In applications where the output buffer is reused without being cleared, this may lead to disclosure of sensitive data. JNI-based implementations are not affected. This vulnerability is fixed in 1.10.1.

**Product:** Oracle Communications, Oracle Financial Services Applications, Oracle Hyperion, Oracle GoldenGate

**Component:** Security (lz4-java) **Affected:** 15.0.0.0-15.0.1.0, 15.1.0.0-15.2.0.0

CWE-201

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (commit tier): https://github.com/yawkat/lz4-java/commit/33d180cb70c4d93c80fb0dc3ab3002f457e93840. ARMR can derive a patch from the linked commit.

## CVE-2026-34309 HIGH CVSS 8.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.61-8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools...

**Product:** Oracle PeopleSoft **Component:** Security **Affected:** 8.61-8.62

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-35243 HIGH CVSS 7.8 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Application Development Framework (ADF) executes to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in takeover of Oracle Application Development Framework (ADF). CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and...

**Product:** Oracle Fusion Middleware **Component:** ADF Faces **Affected:** 12.2.1.4.0, 14.1.2.0.0

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2025-5115 HIGH CVSS 7.7 PATCH-FEASIBLE

In Eclipse Jetty, versions <=9.4.57, <=10.0.25, <=11.0.25, <=12.0.21, <=12.1.0.alpha2, an HTTP/2 client may trigger the server to send RST_STREAM frames, for example by sending frames that are malformed or that should not be sent in a particular stream state, therefore forcing the server to consume resources such as CPU and memory. For example, a client can open a stream and then send WINDOW_UPDATE frames with window size increment of 0, which is illegal. Per specification https://www.rfc-editor.org/rfc/rfc9113.html#name-window_update , the server should send a RST_STREAM frame. The client...

**Product:** Oracle Communications, Oracle Financial Services Applications, Oracle REST Data Services

**Component:** Automated Test Suite (Eclipse Jetty) **Affected:** 25.1.201, 25.2.100

CWE-400 CWE-770

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (pr tier): https://github.com/jetty/jetty.project/pull/13449. ARMR can derive a patch from the linked commit.

## CVE-2026-34310 HIGH CVSS 7.5 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure...

**Product:** Oracle Financial Services Applications **Component:** Platform **Affected:** 8.0.7.9, 8.0.8.7, 8.1.2.5

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34305 HIGH CVSS 7.5 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/...

**Product:** Oracle Fusion Middleware **Component:** Web Services

**Affected:** 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0

CWE-200

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34290 HIGH CVSS 7.5 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Identity Manager Connector. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

**Product:** Oracle Fusion Middleware **Component:** Core **Affected:** 12.2.1.4.0

CWE-400

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34282 HIGH CVSS 7.5 PATCH-FEASIBLE

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in...

**Product:** Oracle Java SE **Component:** Networking

**Affected:** Oracle Java SE: 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18, 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17

CWE-400

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: Red Hat published an advisory (RHSA-2026:11403) confirming a fix exists; the linked Bugzilla ticket (https://bugzilla.redhat.com/show_bug.cgi?id=2460044) traces to the upstream OpenJDK source patch ARMR can derive a rule from.

---

## CVE-2026-33870 HIGH CVSS 7.5 NO-EXPLOIT-DISCLOSURE

Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.132.Final and 4.2.10.Final, Netty incorrectly parses quoted strings in HTTP/1.1 chunked transfer encoding extension values, enabling request smuggling attacks. Versions 4.1.132.Final and 4.2.10.Final fix the issue.

**Product:** Oracle Communications, Oracle Database Server **Component:** Install (Netty) **Affected:** 25.1.200

CWE-444

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

---

## CVE-2026-24734 HIGH CVSS 7.5 NO-EXPLOIT-DISCLOSURE

Improper Input Validation vulnerability in Apache Tomcat Native, Apache Tomcat. When using an OCSP responder, Tomcat Native (and Tomcat's FFM port of the Tomcat Native code) did not complete verification or freshness checks on the OCSP response which could allow certificate revocation to be bypassed. This issue affects Apache Tomcat Native:  from 1.3.0 through 1.3.4, from 2.0.0 through 2.0.11; Apache Tomcat: from 11.0.0-M1 through 11.0.17, from 10.1.0-M7 through 10.1.51, from 9.0.83 through 9.0.114. The following versions were EOL at the time the CVE was created but are known to be...

**Product:** Oracle Hospitality Applications, Oracle Commerce, Oracle Communications, Oracle Utilities Applications

**Component:** Next-Gen SPMS (Apache Tomcat) **Affected:** 23.1.5-23.3.0

CWE-20

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-22016 HIGH CVSS 7.5 MITIGATED-BY-PATCH-RULE

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can...

**Product:** Oracle Java SE **Component:** JAXP

**Affected:** Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18, 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17

CWE-200 CWE-502

**Why this status:** `patch-file-present` An ARMR patch file is present for this CVE (live patch-tree scan); overrides the stored classification "MITIGATED-BY-SECURE-RULE", which predates the patch.

**ARMR:** CVE-2026-22016.armr (https://github.com/waratek/java-patches/blob/develop/vcpu/2026/Q2-April/CVE-2026-22016/patch/2.6/CVE-2026-22016.armr) (spec 2.6)

· last touched 2026-06-18 (b865e807) *JP-588 removed all trailing spaces in armr files*

## CVE-2026-22010 HIGH CVSS 7.5 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure...

**Product:** Oracle Financial Services Applications **Component:** Platform **Affected:** 8.0.7.9, 8.0.8.7, 8.1.2.5

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-21452 HIGH CVSS 7.5 MITIGATED-BY-SECURE-RULE

MessagePack for Java is a serializer implementation for Java. A denial-of-service vulnerability exists in versions prior to 0.9.11 when deserializing .msgpack files containing EXT32 objects with attacker-controlled payload lengths. While MessagePack-Java parses extension headers lazily, it later trusts the declared EXT payload length when materializing the extension data. When ExtensionValue.getData() is invoked, the library attempts to allocate a byte array of the declared length without enforcing any upper bound. A malicious .msgpack file of only a few bytes can therefore trigger unbounded...

**Product:** Oracle Communications **Component:** Configuration (MessagePack) **Affected:** 25.1.200

CWE-400 CWE-789

**Why this status:** `secure-rule-match` Promoted to MITIGATED-BY-SECURE-RULE: this CVE's description identifies a deserialization vulnerability that can be mitigated by an ARMR deserialization security rule at the JVM level, without requiring a CVE-specific patch. Matched by description (no specific CWE was assigned by NVD).

### CVE-2025-67635 HIGH CVSS 7.5 PATCH-FEASIBLE

Jenkins 2.540 and earlier, LTS 2.528.2 and earlier does not properly close HTTP-based CLI connections when the connection stream becomes corrupted, allowing unauthenticated attackers to cause a denial of service.

**Product:** Oracle Communications **Component:** Install (Jenkins) **Affected:** 25.1.100, 25.1.200

CWE-404

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.jenkins-ci.main:jenkins-core, org.jenkins-ci.main:cli). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

### CVE-2025-64775 HIGH CVSS 7.5 PATCH-FEASIBLE

Denial of Service vulnerability in Apache Struts, file leak in multipart request processing causes disk exhaustion. This issue affects Apache Struts: from 2.0.0 through 6.7.0, from 7.0.0 through 7.0.3. Users are recommended to upgrade to version 6.8.0 or 7.1.1, which fixes the issue.

**Product:** Oracle Hyperion **Component:** Installation and Configuration (Apache Struts) **Affected:** 11.2.24.0.000

CWE-459

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.struts:struts2-core). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

### CVE-2025-48976 HIGH CVSS 7.5 PATCH-FEASIBLE

Allocation of resources for multipart headers with insufficient limits enabled a DoS vulnerability in Apache Commons FileUpload. This issue affects Apache Commons FileUpload: from 1.0 before 1.6; from 2.0.0-M1 before 2.0.0-M4. Users are recommended to upgrade to versions 1.6 or 2.0.0-M4, which fix the issue.

**Product:** Oracle Communications, Oracle Financial Services Applications, Oracle Adapter for Eclipse RDF4J

**Component:** Platform (Apache Commons FileUpload) **Affected:** 24.2.1

CWE-770

---

### CVE-2025-41253 HIGH CVSS 7.5 PATCH-FEASIBLE

The following versions of Spring Cloud Gateway Server Webflux may be vulnerable to the ability to expose environment variables and system properties to attackers. An application should be considered vulnerable when all the following are true: * The application is using Spring Cloud Gateway Server Webflux (Spring Cloud Gateway Server WebMVC is not vulnerable). * An admin or untrusted third party using Spring Expression Language (SpEL) to access environment variables or system properties via routes. * An untrusted third party could create a route that uses SpEL to access environment...

**Product:** Oracle Communications **Component:** Install (Spring Cloud Gateway) **Affected:** 24.2.4

CWE-917

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.springframework.cloud:spring-cloud-gateway-server-webflux). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2025-41249 HIGH CVSS 7.5 PATCH-FEASIBLE

The Spring Framework annotation detection mechanism may not correctly resolve annotations on methods within type hierarchies with a parameterized super type with unbounded generics. This can be an issue if such annotations are used for authorization decisions. Your application may be affected by this if you are using Spring Security's @EnableMethodSecurity feature. You are not affected by this if you are not using @EnableMethodSecurity or if you do not use security annotations on methods in generic superclasses or generic interfaces. This CVE is published in conjunction with...

**Product:** Oracle Communications, Oracle Financial Services Applications, Oracle Fusion Middleware, Oracle Enterprise Manager

**Component:** Install (Spring Framework) **Affected:** 24.2.1

CWE-285 CWE-863

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.springframework:spring-core). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

## CVE-2025-41248 HIGH CVSS 7.5 PATCH-FEASIBLE

The Spring Security annotation detection mechanism may not correctly resolve annotations on methods within type hierarchies with a parameterized super type with unbounded generics. This can be an issue when using @PreAuthorize and other method security annotations, resulting in an authorization bypass. Your application may be affected by this if you are using Spring Security's @EnableMethodSecurity feature. You are not affected by this if you are not using @EnableMethodSecurity or if you do not use security annotations on methods in generic superclasses or generic interfaces. This CVE...

**Product:** Oracle Communications, Oracle Financial Services Applications **Component:** Signaling (Spring Security)

**Affected:** 25.1.204

CWE-289 CWE-863

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.springframework.security:spring-security-core). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

## CVE-2025-27820 HIGH CVSS 7.5 PATCH-FEASIBLE

A bug in PSL validation logic in Apache HttpClient 5.4.x disables domain checks, affecting cookie management and host name verification. Discovered by the Apache HttpClient team. Fixed in the 5.4.3 release

**Product:** Oracle Financial Services Applications **Component:** Platform (Apache HttpClient)

**Affected:** 8.0.7.9, 8.0.8.7, 8.1.2.5

CWE-295

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (pr tier): https://github.com/apache/httpcomponents-client/pull/574. ARMR can derive a patch from the linked commit.

### CVE-2025-27817 HIGH CVSS 7.5 PATCH-FEASIBLE

A possible arbitrary file read and SSRF vulnerability has been identified in Apache Kafka Client. Apache Kafka Clients accept configuration data for setting the SASL/OAUTHBEARER connection with the brokers, including "sasl.oauthbearer.token.endpoint.url" and "sasl.oauthbearer.jwks.endpoint.url". Apache Kafka allows clients to read an arbitrary file and return the content in the error log, or sending requests to an unintended location. In applications where Apache Kafka Clients configurations can be specified by an untrusted party, attackers may use the "sasl.oauthbearer.token.endpoint.url"...

**Product:** Oracle Financial Services Applications, Oracle Siebel CRM **Component:** Base (Apache Kafka)

**Affected:** 14.5.0.0.0-14.8.0.0.0

CWE-918

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.kafka:kafka-clients). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

### CVE-2025-24970 HIGH CVSS 7.5 PATCH-FEASIBLE

Netty, an asynchronous, event-driven network application framework, has a vulnerability starting in version 4.1.91.Final and prior to version 4.1.118.Final. When a special crafted packet is received via SslHandler it doesn't correctly handle validation of such a packet in all cases which can lead to a native crash. Version 4.1.118.Final contains a patch. As workaround its possible to either disable the usage of the native SSLEngine or change the code manually.

**Product:** Oracle Analytics **Component:** Analytics Server (Netty) **Affected:** 8.2.0.0.0

CWE-20

---

### CVE-2025-1948 HIGH CVSS 7.5 PATCH-FEASIBLE

In Eclipse Jetty versions 12.0.0 to 12.0.16 included, an HTTP/2 client can specify a very large value for the HTTP/2 settings parameter SETTINGS_MAX_HEADER_LIST_SIZE. The Jetty HTTP/2 server does not perform validation on this setting, and tries to allocate a ByteBuffer of the specified capacity to encode HTTP responses, likely resulting in OutOfMemoryError being thrown, or even the JVM process exiting.

**Product:** Oracle Financial Services Applications **Component:** Configuration (Eclipse Jetty)

**Affected:** 14.5.0.0.0-14.8.0.0.0

CWE-400

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.eclipse.jetty.http2:jetty-http2-common). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

### CVE-2024-29857 HIGH CVSS 7.5 PATCH-FEASIBLE

An issue was discovered in ECCurve.java and ECCurve.cs in Bouncy Castle Java (BC Java) before 1.78, BC Java LTS before 2.73.6, BC-FJA before 1.0.2.5, and BC C# .Net before 2.3.1. Importing an EC certificate with crafted F2m parameters can lead to excessive CPU consumption during the evaluation of the curve parameters.

**Product:** Oracle Fusion Middleware **Component:** B2B Engine (Bouncy Castle Java Library) **Affected:** 12.2.1.4.0

CWE-125 CWE-400

### CVE-2024-29371 HIGH CVSS 7.5 PATCH-FEASIBLE

In jose4j before 0.9.6, an attacker can cause a Denial-of-Service (DoS) condition by crafting a malicious JSON Web Encryption (JWE) token with an exceptionally high compression ratio. When this token is processed by the server, it results in significant memory allocation and processing time during decompression.

**Product:** Oracle Siebel CRM **Component:** Event Publish and Subscribe (jose4j) **Affected:** 17.0-26.2

CWE-1259

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: Red Hat published an advisory (RHSA-2024:5479) confirming a fix exists; the linked Bugzilla ticket (https://bugzilla.redhat.com/show_bug.cgi?id=2423194) points to the upstream OpenJDK source patch. A rule may be derivable from it — this has not been confirmed and requires reviewing the actual change.

### CVE-2023-52428 HIGH CVSS 7.5 PATCH-FEASIBLE

In Connect2id Nimbus JOSE+JWT before 9.37.2, an attacker can cause a denial of service (resource consumption) via a large JWE p2c header value (aka iteration count) for the PasswordBasedDecrypter (PBKDF2) component.

**Product:** Oracle Analytics **Component:** Platform Security (Nimbus JOSE+JWT) **Affected:** 7.6.0.0.0, 8.2.0.0.0

CWE-770 CWE-400

### CVE-2023-26464 HIGH CVSS 7.5 MITIGATED-BY-PATCH-RULE

** UNSUPPORTED WHEN ASSIGNED ** When using the Chainsaw or SocketAppender components with Log4j 1.x on JRE less than 1.7, an attacker that manages to cause a logging entry involving a specially-crafted (ie, deeply nested) hashmap or hashtable (depending on which logging component is in use) to be processed could exhaust the available memory in the virtual machine and achieve Denial of Service when the object is deserialized. This issue affects Apache Log4j before 2. Affected users are recommended to update to Log4j 2.x. NOTE: This vulnerability only affects products that are no longer...

**Product:** Oracle Siebel CRM **Component:** Server Infrastructure (Apache Log4j) **Affected:** 17.0-25.11

CWE-502 CWE-400

**Why this status:** `ARMR patch` CVE is covered by a multi-CVE ARMR patch rule

**ARMR:** CVE-2021-45046.armr (https://github.com/waratek/java-patches/blob/develop/rules/libraries/apache/log4j/CVE-2021-45046/patch/2.6/CVE-2021-45046.armr) (spec 2.6)

### CVE-2022-45688 HIGH CVSS 7.5 PATCH-FEASIBLE

A stack overflow in the XML.toJSONObject component of hutool-json v5.8.10 allows attackers to cause a Denial of Service (DoS) via crafted JSON or XML data.

**Product:** Oracle Siebel CRM **Component:** Data Archival (Quartz) **Affected:** 17.0-25.11

CWE-787

### CVE-2021-0341 HIGH CVSS 7.5 PATCH-FEASIBLE

In verifyHostName of OkHostnameVerifier.java, there is a possible way to accept a certificate for the wrong domain due to improperly used crypto. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-171980069

**Product:** Oracle Communications **Component:** Install (OkHttp) **Affected:** 25.1.200

CWE-295

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: com.squareup.okhttp3:okhttp). OSV.dev confirms the advisory and the source is publicly available, so a patch may be feasible — this has not been confirmed and requires reviewing the diff between the affected and fixed versions.

---

### CVE-2025-27821 HIGH CVSS 7.3 PATCH-FEASIBLE

Out-of-bounds Write vulnerability in Apache Hadoop HDFS native client. This issue affects Apache Hadoop: from 3.2.0 before 3.4.2. Users are recommended to upgrade to version 3.4.2, which fixes the issue.

**Product:** Oracle Communications, Oracle Financial Services Applications **Component:** Core (Apache Hadoop)

**Affected:** 6.1.1-7.0.0

CWE-787

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.hadoop:hadoop-hdfs-native-client). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

### CVE-2026-34292 HIGH CVSS 7.2 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).

**Product:** Oracle Fusion Middleware **Component:** Core **Affected:** 12.2.1.4.0, 14.1.1.0.0

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

---

### CVE-2024-13009 HIGH CVSS 7.2 PATCH-FEASIBLE

In Eclipse Jetty versions 9.4.0 to 9.4.56 a buffer can be incorrectly released when confronted with a gzip error when inflating a request body. This can result in corrupted and/or inadvertent sharing of data between requests.

**Product:** Oracle Fusion Middleware **Component:** Third Party (jackson-databind) **Affected:** 12.2.1.4.0

CWE-404

## CVE-2025-46762 HIGH CVSS 7.1 PATCH-FEASIBLE

Schema parsing in the parquet-avro module of Apache Parquet 1.15.0 and previous versions allows bad actors to execute arbitrary code. While 1.15.1 introduced a fix to restrict untrusted packages, the default setting of trusted packages still allows malicious classes from these packages to be executed. The exploit is only applicable if the client code of parquet-avro uses the "specific" or the "reflect" models deliberately for reading Parquet files. ("generic" model is not impacted) Users are recommended to upgrade to 1.15.2 or set the system property "org.apache.parquet.avro.SERIALIZABLE_PA...

**Product:** Oracle Analytics **Component:** Platform Security (Apache Parquet Java) **Affected:** 8.2.0.0.0

CWE-73

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.parquet:parquet-avro). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2026-21939 HIGH CVSS 7.0 NO-EXPLOIT-DISCLOSURE

Vulnerability in the SQLcl component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.0. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where SQLcl executes to compromise SQLcl. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of SQLcl. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).

**Product:** Oracle Fusion Middleware **Component:** Oracle Database Client for Fusion Middleware

**Affected:** 14.1.2.0.0

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2025-58057 MEDIUM CVSS 6.9 PATCH-FEASIBLE

Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In netty-codec-compression versions 4.1.124.Final and below, and netty-codec versions 4.2.4.Final and below, when supplied with specially crafted input, BrotliDecoder and certain other decompression decoders will allocate a large number of reachable byte buffers, which can lead to denial of service. BrotliDecoder.decompress has no limit in how often it calls pull, decompressing data 64K bytes at a time. The buffers are saved in the output list,...

**Product:** Oracle E-Business Suite, Oracle Analytics, Oracle Communications, Oracle Financial Services Applications, Oracle Siebel CRM

**Component:** ECC Core (Netty) **Affected:** 15.0

CWE-409

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (commit tier): https://github.com/netty/netty/commit/9d804c54ce962408ae6418255a83a13924f7145d. ARMR can derive a patch from the linked commit.

## CVE-2025-35036 MEDIUM CVSS 6.9 PATCH-FEASIBLE

Hibernate Validator before 6.2.0 and 7.0.0, by default and depending how it is used, may interpolate user-supplied input in a constraint violation message with Expression Language. This could allow an attacker to access sensitive information or execute arbitrary Java code. Hibernate Validator as of 6.2.0 and 7.0.0 no longer interpolates custom constraint violation messages with Expression Language and strongly recommends not allowing user-supplied input in constraint violation messages. CVE-2020-5245 and CVE-2025-4428 are examples of related, downstream vulnerabilities involving Expression...

**Product:** Oracle Fusion Middleware **Component:** Third Party (Validator) **Affected:** 12.2.1.4.0, 14.1.2.0.0

CWE-94

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (commit tier): https://github.com/hibernate/hibernate-validator/commit/05f795bb7cf18856004f40e5042709e550ed0d6e. ARMR can derive a patch from the linked commit.

## CVE-2026-34325 MEDIUM CVSS 6.8 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Financial Services Analytical Applications Infrastructure executes to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker. Successful attacks...

**Product:** Oracle Financial Services Applications **Component:** User Interface **Affected:** 8.0.7.9, 8.0.8.7, 8.1.2.5

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34314 MEDIUM CVSS 6.8 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Analytical Applications...

**Product:** Oracle Financial Services Applications **Component:** Platform **Affected:** 8.0.7.9, 8.0.8.7, 8.1.2.5

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34277 MEDIUM CVSS 6.6 NO-EXPLOIT-DISCLOSURE

Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Fluid Core). Supported versions that are affected are 8.61-8.62. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible...

**Product:** Oracle PeopleSoft **Component:** Fluid Core **Affected:** 8.61-8.62

CWE-284 CWE-400

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34315 MEDIUM CVSS 6.5 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS...

**Product:** Oracle Fusion Middleware **Component:** Web Services

**Affected:** 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0, 15.1.1.0.0

CWE-285 CWE-601

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34313 MEDIUM CVSS 6.5 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Platform). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financial Services Analytical Applications Infrastructure...

**Product:** Oracle Financial Services Applications **Component:** Platform **Affected:** 8.0.7.9, 8.0.8.7, 8.1.2.5

CWE-200

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2025-67735 MEDIUM CVSS 6.5 PATCH-FEASIBLE

Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.129.Final and 4.2.8.Final, the `io.netty.handler.codec.http.HttpRequestEncoder` has a CRLF injection with the request URI when constructing a request. This leads to request smuggling when `HttpRequestEncoder` is used without proper sanitization of the URI. Any application / framework using `HttpRequestEncoder` can be subject to be abused to perform request smuggling using CRLF injection. Versions 4.1.129.Final and 4.2.8.Final fix the issue.

**Product:** Oracle Financial Services Applications, Oracle GoldenGate **Component:** Infrastructure (Netty)

**Affected:** 14.8.1.0.0

CWE-93

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: io.netty:netty-codec-http). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2025-46392 MEDIUM CVSS 6.5 PATCH-FEASIBLE

Uncontrolled Resource Consumption vulnerability in Apache Commons Configuration 1.x. There are a number of issues in Apache Commons Configuration 1.x that allow excessive resource consumption when loading untrusted configurations or using unexpected usage patterns. The Apache Commons Configuration team does not intend to fix these issues in 1.x. Apache Commons Configuration 1.x is still safe to use in scenario's where you only load trusted configurations. Users that load untrusted configurations or give attackers control over usage patterns are recommended to upgrade to the 2.x version...

**Product:** Oracle Financial Services Applications, Oracle Fusion Middleware

**Component:** Common Core (Apache Commons Configuration) **Affected:** 14.5.0.0.0-14.8.0.0.0

CWE-400

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: commons-configuration:commons-configuration). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2023-20863 MEDIUM CVSS 6.5 PATCH-FEASIBLE

In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.

**Product:** Oracle Financial Services Applications **Component:** Logger (Spring Framework) **Affected:** 1.0.2.1

CWE-400 CWE-917 CWE-770

## CVE-2026-35252 MEDIUM CVSS 6.4 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Security Service product of Oracle Fusion Middleware (component: C Oracle SSL API). Supported versions that are affected are 12.2.1.4.0 and 12.1.3.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Security Service. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Security Service accessible data as well as...

**Product:** Oracle Fusion Middleware **Component:** C Oracle SSL API **Affected:** 12.2.1.4.0, 12.1.3.0.0

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2025-8916 MEDIUM CVSS 6.3 PATCH-FEASIBLE

Allocation of Resources Without Limits or Throttling vulnerability in Legion of the Bouncy Castle Inc. BC Java bcpkix on All (API modules), Legion of the Bouncy Castle Inc. BC Java bcprov on All (API modules), Legion of the Bouncy Castle Inc. BCPKIX FIPS bcpkix-fips on All (API modules) allows Excessive Allocation. This vulnerability is associated with program files https://github.Com/bcgit/bc-java/blob/main/pkix/src/main/java/org/bouncycastle/pkix/jcajce/PKIXCertPathReviewer.Java, https://github.Com/bcgit/bc-java/blob/main/prov/src/main/java/org/bouncycastle/x509/PKIXCertPathReviewer.Java. T...

**Product:** Oracle Fusion Middleware, Oracle GoldenGate

**Component:** Thirdparty Patch (Bouncy Castle Java Library) **Affected:** 14.1.2.0.0

CWE-770

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.bouncycastle:bcpkix-jdk15on, org.bouncycastle:bcpkix-jdk15to18, org.bouncycastle:bcpkix-jdk18on, org.bouncycastle:bcpkix-fips). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2025-68161 MEDIUM CVSS 6.3 PATCH-FEASIBLE

The Socket Appender in Apache Log4j Core versions 2.0-beta9 through 2.25.2 does not perform TLS hostname verification of the peer certificate, even when the verifyHostName https://logging.apache.org/log4j/2.x/manual/appenders/network.html#SslConfiguration-attr-verifyHostName configuration attribute or the log4j2.sslVerifyHostName https://logging.apache.org/log4j/2.x/manual/systemproperties.html#log4j2.sslVerifyHostName system property is set to true. This issue may allow a man-in-the-middle attacker to intercept or redirect log traffic under the following conditions: * The attacker...

**Product:** Oracle E-Business Suite, Oracle Analytics, Oracle Retail Applications, Oracle Communications, Oracle Financial Services Applications, Oracle Life Science Applications, Oracle Utilities Applications, Oracle Fusion Middleware, Oracle Construction and Engineering, Oracle Enterprise Manager, Oracle GoldenGate, Oracle PeopleSoft, Oracle Siebel CRM, Oracle Supply Chain

**Component:** ECC Core (Apache Log4j) **Affected:** 15.0

CWE-297 CWE-295

## CVE-2021-28168 MEDIUM CVSS 6.2 PATCH-FEASIBLE

Eclipse Jersey 2.28 to 2.33 and Eclipse Jersey 3.0.0 to 3.0.1 contains a local information disclosure vulnerability. This is due to the use of the File.createTempFile which creates a file inside of the system temporary directory with the permissions: -rw-r--r--. Thus the contents of this file are viewable by all other users locally on the system. As such, if the contents written is security sensitive, it can be disclosed to other local users.

**Product:** Oracle Analytics, Oracle Financial Services Applications **Component:** Platform Security (Eclipse Jersey)

**Affected:** 7.6.0.0.0, 8.2.0.0.0

CWE-378 CWE-379 CWE-668 CWE-732

## CVE-2026-34284 MEDIUM CVSS 6.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Business Process Management Suite product of Oracle Fusion Middleware (component: Human workflow 11g+). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Process Management Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Process Management Suite, attacks may significantly impact additional products (scope change). Successful attacks...

**Product:** Oracle Fusion Middleware **Component:** Human workflow 11g+ **Affected:** 12.2.1.4.0, 14.1.2.0.0

CWE-284 CWE-601

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34283 MEDIUM CVSS 6.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: Identity Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Identity Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized...

**Product:** Oracle Fusion Middleware **Component:** Identity Console **Affected:** 12.2.1.4.0, 14.1.2.0.0

CWE-284 CWE-601

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34269 MEDIUM CVSS 6.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.61-8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update,...

**Product:** Oracle PeopleSoft **Component:** Portal **Affected:** 8.61-8.62

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

---

## CVE-2023-46750 MEDIUM CVSS 6.1 PATCH-FEASIBLE

URL Redirection to Untrusted Site ('Open Redirect') vulnerability when "form" authentication is used in Apache Shiro. Mitigation: Update to Apache Shiro 1.13.0+ or 2.0.0-alpha-4+.

**Product:** Oracle Adapter for Eclipse RDF4J **Component:** Jena adapter (Apache Shiro) **Affected:** 24.1.0

CWE-601

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.shiro:shiro-web). OSV.dev confirms the advisory and the source is publicly available, so a patch may be feasible — this has not been confirmed and requires reviewing the diff between the affected and fixed versions.

---

## CVE-2025-7962 MEDIUM CVSS 6.0 PATCH-FEASIBLE

In Jakarta Mail 2.0.2 it is possible to preform a SMTP Injection by utilizing the \r and \n UTF-8 characters to separate different messages.

**Product:** Oracle Retail Applications, Oracle Siebel CRM **Component:** Point of Sale (Jakarta Mail)

**Affected:** 21.0.5, 22.0.3

CWE-147

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.eclipse.angus:smtp). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2026-34294 MEDIUM CVSS 5.9 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Microsoft Active Directory). The supported version that is affected is 12.2.1.4.0. Difficult to exploit vulnerability allows low privileged attacker with network access via LDAP to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized read access to a subset of Oracle Identity Manager...

**Product:** Oracle Fusion Middleware **Component:** Microsoft Active Directory **Affected:** 12.2.1.4.0

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34289 MEDIUM CVSS 5.9 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).

**Product:** Oracle Fusion Middleware **Component:** Core **Affected:** 12.2.1.4.0

CWE-306

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34288 MEDIUM CVSS 5.9 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). The supported version that is affected is 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).

**Product:** Oracle Fusion Middleware **Component:** Core **Affected:** 12.2.1.4.0

CWE-306

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

### CVE-2025-41242 MEDIUM CVSS 5.9 MITIGATED-BY-SECURE-RULE

Spring Framework MVC applications can be vulnerable to a “Path Traversal Vulnerability” when deployed on a non-compliant Servlet container. An application can be vulnerable when all the following are true: * the application is deployed as a WAR or with an embedded Servlet container * the Servlet container does not reject suspicious sequences https://jakarta.ee/specifications/servlet/6.1/jakarta-servlet-spec-6.1.html#uri-path-canonicalization * the application serves static resources https://docs.spring.io/spring-framework/reference/web/webmvc/mvc-config/static-resources.html#...

**Product:** Oracle E-Business Suite **Component:** ECC Core (Spring Framework) **Affected:** 15.0

CWE-22

**Why this status:** `secure-rule-match` Promoted to MITIGATED-BY-SECURE-RULE: this CVE's weakness (CWE-22: Path Traversal) can be mitigated by an ARMR path-traversal security rule that blocks this class of attack at the JVM level, without requiring a CVE-specific patch.

---

### CVE-2024-8184 MEDIUM CVSS 5.9 PATCH-FEASIBLE

There exists a security vulnerability in Jetty's ThreadLimitHandler.getRemote() which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack. By repeatedly sending crafted requests, attackers can trigger OutofMemory errors and exhaust the server's memory.

**Product:** Oracle Communications **Component:** Platform (Eclipse Jetty) **Affected:** 24.2.1

CWE-400 CWE-770

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (pr tier): https://github.com/jetty/jetty.project/pull/11723. A patch may be feasible — this has not been confirmed and requires reviewing the linked change.

---

### CVE-2023-34453 MEDIUM CVSS 5.9 PATCH-FEASIBLE

snappy-java is a fast compressor/decompressor for Java. Due to unchecked multiplications, an integer overflow may occur in versions prior to 1.1.10.1, causing a fatal error. The function `shuffle(int[] input)` in the file `BitShuffle.java` receives an array of integers and applies a bit shuffle on it. It does so by multiplying the length by 4 and passing it to the natively compiled shuffle function. Since the length is not tested, the multiplication by four can cause an integer overflow and become a smaller value than the true size, or even zero or negative. In the case of a negative value,...

**Product:** Oracle Communications **Component:** Platform (Snappy) **Affected:** 24.2.1

CWE-190

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (commit tier): https://github.com/xerial/snappy-java/commit/820e2e074c58748b41dbd547f4edba9e108ad905. A patch may be feasible — this has not been confirmed and requires reviewing the linked change.

---

### CVE-2023-1436 MEDIUM CVSS 5.9 PATCH-FEASIBLE

An infinite recursion is triggered in Jettison when constructing a JSONArray from a Collection that contains a self-reference in one of its elements. This leads to a StackOverflowError exception being thrown.

**Product:** Oracle Siebel CRM **Component:** REST (Jettison) **Affected:** 17.0-26.2

CWE-674

## CVE-2025-53864 MEDIUM CVSS 5.8 PATCH-FEASIBLE

Connect2id Nimbus JOSE + JWT 10.0.x before 10.0.2 and 9.37.x before 9.37.4 allows a remote attacker to cause a denial of service via a deeply nested JSON object supplied in a JWT claim set, because of uncontrolled recursion. NOTE: this is independent of the Gson 2.11.0 issue because the Connect2id product could have checked the JSON object nesting depth, regardless of what limits (if any) were imposed by Gson.

**Product:** Oracle Fusion Middleware **Component:** Security (Nimbus JOSE+JWT) **Affected:** 12.2.1.4.0, 14.1.2.0.0

CWE-674

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (commit tier): https://bitbucket.org/connect2id/nimbus-jose-jwt/commits/f7fb882cc08f027c9ceb874acec3b51c6222861c. ARMR can derive a patch from the linked commit.

---

## CVE-2025-48795 MEDIUM CVSS 5.6 PATCH-FEASIBLE

Apache CXF stores large stream based messages as temporary files on the local filesystem. A bug was introduced which means that the entire temporary file is read into memory and then logged. An attacker might be able to exploit this to cause a denial of service attack by causing an out of memory exception. In addition, it is possible to configure CXF to encrypt temporary files to prevent sensitive credentials from being cached unencrypted on the local filesystem, however this bug means that the cached files are written out to logs unencrypted. Users are recommended to upgrade to versions...

**Product:** Oracle Communications, Oracle Construction and Engineering **Component:** Security (Apache CXF)

**Affected:** 25.1.200

CWE-400

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.cxf:cxf-core). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

## CVE-2025-27636 MEDIUM CVSS 5.6 PATCH-FEASIBLE

Bypass/Injection vulnerability in Apache Camel components under particular conditions. This issue affects Apache Camel: from 4.10.0 through <= 4.10.1, from 4.8.0 through <= 4.8.4, from 3.10.0 through <= 3.22.3. Users are recommended to upgrade to version 4.10.2 for 4.10.x LTS, 4.8.5 for 4.8.x LTS and 3.22.4 for 3.x releases. This vulnerability is present in Camel's default incoming header filter, that allows an attacker to include Camel specific headers that for some Camel components can alter the behaviours such as the camel-bean component, to call another method on the bean, than was...

**Product:** Oracle Financial Services Applications **Component:** Platform (Apache Camel)

**Affected:** 14.5.0.0.0-14.8.0.0.0

CWE-178

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.camel:camel-support). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2025-66453 MEDIUM CVSS 5.5 PATCH-FEASIBLE

Rhino is an open-source implementation of JavaScript written entirely in Java. Prior to 1.8.1, 1.7.15.1, and 1.7.14.1, when an application passed an attacker controlled float poing number into the toFixed() function, it might lead to high CPU consumption and a potential Denial of Service. Small numbers go through this call stack: NativeNumber.numTo > DToA.JS_dtostr > DToA.JS_dtoa > DToA.pow5mult where pow5mult attempts to raise 5 to a ridiculous power. This vulnerability is fixed in 1.8.1, 1.7.15.1, and 1.7.14.1.

**Product:** Oracle REST Data Services **Component:** REST Services (Rhino)

**Affected:** 24.2.0, 24.2.1, 24.3.0, 24.3.1, 24.4.0, 25.1.1, 25.2.0, 25.2.1, 25.2.2, 25.2.3, 25.3.0, 25.3.1, 25.4.0

CWE-400

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.mozilla:rhino). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

## CVE-2025-59419 MEDIUM CVSS 5.5 MITIGATED-BY-SECURE-RULE

Netty is an asynchronous, event-driven network application framework. In versions prior to 4.1.128.Final and 4.2.7.Final, the SMTP codec in Netty contains an SMTP command injection vulnerability due to insufficient input validation for Carriage Return (\r) and Line Feed (\n) characters in user-supplied parameters. The vulnerability exists in io.netty.handler.codec.smtp.DefaultSmtpRequest, where parameters are directly concatenated into the SMTP command string without sanitization. When methods such as SmtpRequests.rcpt(recipient) are called with a malicious string containing CRLF sequences,...

**Product:** Oracle Analytics **Component:** Platform Security (netty-codec-smtp) **Affected:** 8.2.0.0.0

CWE-93 CWE-78

**Why this status:** `secure-rule-match` Promoted to MITIGATED-BY-SECURE-RULE: this CVE's weakness (CWE-78: OS Command Injection) can be mitigated by an ARMR command-injection security rule that blocks this class of attack at the JVM level, without requiring a CVE-specific patch.

---

## CVE-2023-2976 MEDIUM CVSS 5.5 MITIGATED-BY-ENVIRONMENT

Use of Java's default temporary directory for file creation in `FileBackedOutputStream` in Google Guava versions 1.0 to 31.1 on Unix systems and Android Ice Cream Sandwich allows other users and apps on the machine with access to the default Java temporary directory to be able to access the files created by the class. Even though the security vulnerability is fixed in version 32.0.0, we recommend using version 32.0.1 as version 32.0.0 breaks some functionality under Windows.

**Product:** Oracle Fusion Middleware **Component:** Oracle MFT Installer (Google Guava) **Affected:** 12.2.1.4.0

CWE-552 CWE-379

## CVE-2020-17521 MEDIUM CVSS 5.5 MITIGATED-BY-SECURE-RULE

Apache Groovy provides extension methods to aid with creating temporary directories. Prior to this fix, Groovy's implementation of those extension methods was using a now superseded Java JDK method call that is potentially not secure on some operating systems in some contexts. Users not using the extension methods mentioned in the advisory are not affected, but may wish to read the advisory for further details. Versions Affected: 2.0 to 2.4.20, 2.5.0 to 2.5.13, 3.0.0 to 3.0.6, and 4.0.0-alpha-1. Fixed in versions 2.4.21, 2.5.14, 3.0.7, 4.0.0-alpha-2.

**Product:** Oracle Utilities Applications **Component:** Security (Apache Groovy)

**Affected:** 4.3.0.5.0-4.3.0.6.0, 4.4.0.0.0-4.4.0.3.0

CWE-379

## CVE-2026-35232 MEDIUM CVSS 5.4 NO-EXPLOIT-DISCLOSURE

Vulnerability in Oracle Fusion Middleware (component: Dynamic Monitoring Service). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Fusion Middleware. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Fusion Middleware, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access...

**Product:** Oracle Fusion Middleware **Component:** Dynamic Monitoring Service **Affected:** 12.2.1.4.0, 14.1.2.0.0

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34307 MEDIUM CVSS 5.4 NO-EXPLOIT-DISCLOSURE

Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Workflow). Supported versions that are affected are 8.61-8.62. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized...

**Product:** Oracle PeopleSoft **Component:** Workflow **Affected:** 8.61-8.62

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

### CVE-2026-34273 MEDIUM CVSS 5.3 NO-EXPLOIT-DISCLOSURE

Vulnerability in Oracle GoldenGate (component: Libraries). Supported versions that are affected are 23.4-23.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle GoldenGate. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GoldenGate accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

**Product:** Oracle GoldenGate **Component:** Libraries **Affected:** 23.4-23.10

CWE-200

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

---

### CVE-2026-23903 MEDIUM CVSS 5.3 NO-EXPLOIT-DISCLOSURE

Authentication Bypass by Alternate Name vulnerability in Apache Shiro. This issue affects Apache Shiro: before 2.0.7. Users are recommended to upgrade to version 2.0.7, which fixes the issue. The issue only effects static files. If static files are served from a case-insensitive filesystem, such as default macOS setup, static files may be accessed by varying the case of the filename in the request. If only lower-case (common default) filters are present in Shiro, they may be bypassed this way. Shiro 2.0.7 and later has a new parameters to remediate this issue shiro.ini:...

**Product:** Oracle Communications **Component:** Third Party (Apache Shiro) **Affected:** 9.0.0-9.0.4

CWE-289

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

---

### CVE-2026-22021 MEDIUM CVSS 5.3 PATCH-FEASIBLE

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in...

**Product:** Oracle Java SE **Component:** JSSE

**Affected:** Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18, 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17

CWE-400

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: Red Hat published an advisory (RHSA-2026:11403) confirming a fix exists; the linked Bugzilla ticket (https://bugzilla.redhat.com/show_bug.cgi?id=2460042) traces to the upstream OpenJDK source patch ARMR can derive a rule from.

## CVE-2025-61795 MEDIUM CVSS 5.3 PATCH-FEASIBLE

Improper Resource Shutdown or Release vulnerability in Apache Tomcat. If an error occurred (including exceeding limits) during the processing of a multipart upload, temporary copies of the uploaded parts written to disc were not cleaned up immediately but left for the garbage collection process to delete. Depending on JVM settings, application memory usage and application load, it was possible that space for the temporary copies of uploaded parts would be filled faster than GC cleared it, leading to a DoS. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.11, from 10.1.0-M1...

**Product:** Oracle Communications **Component:** Security (Apache Tomcat) **Affected:** 47.0.0.1.0

CWE-404

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.apache.tomcat:tomcat, org.apache.tomcat:tomcat-catalina, org.apache.tomcat.embed:tomcat-embed-core). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

## CVE-2025-48924 MEDIUM CVSS 5.3 PATCH-FEASIBLE

Uncontrolled Recursion vulnerability in Apache Commons Lang. This issue affects Apache Commons Lang: Starting with commons-lang:commons-lang 2.0 to 2.6, and, from org.apache.commons:commons-lang3 3.0 before 3.18.0. The methods ClassUtils.getClass(...) can throw StackOverflowError on very long inputs. Because an Error is usually not handled by applications and libraries, a StackOverflowError could cause an application to stop. Users are recommended to upgrade to version 3.18.0, which fixes the issue.

**Product:** Oracle Analytics, Oracle Retail Applications, Oracle Financial Services Applications, Oracle JD Edwards, Oracle Utilities Applications, Oracle Fusion Middleware, Oracle GoldenGate, Oracle Siebel CRM, Oracle Database Server

**Component:** BI Publisher Microservice (Apache Commons Lang) **Affected:** 7.6.0.0.0, 8.2.0.0.0

CWE-674

## CVE-2025-31672 MEDIUM CVSS 5.3 PATCH-FEASIBLE

Improper Input Validation vulnerability in Apache POI. The issue affects the parsing of OOXML format files like xlsx, docx and pptx. These file formats are basically zip files and it is possible for malicious users to add zip entries with duplicate names (including the path) in the zip. In this case, products reading the affected file could read different data because 1 of the zip entries with the duplicate name is selected over another but different products may choose a different zip entry. This issue affects Apache POI poi-ooxml before 5.4.0. poi-ooxml 5.4.0 has a check that throws an...

**Product:** Oracle E-Business Suite, Oracle Fusion Middleware **Component:** ECC Core (Apache POI)

**Affected:** 15.0

CWE-20

## CVE-2024-36124 MEDIUM CVSS 5.3 PATCH-FEASIBLE

iq80 Snappy is a compression/decompression library. When uncompressing certain data, Snappy tries to read outside the bounds of the given byte arrays. Because Snappy uses the JDK class `sun.misc.Unsafe` to speed up memory access, no additional bounds checks are performed and this has similar security consequences as out-of-bounds access in C or C++, namely it can lead to non-deterministic behavior or crash the JVM. iq80 Snappy is not actively maintained anymore. As quick fix users can upgrade to version 0.5.

**Product:** Oracle Siebel CRM **Component:** Open Integration (Snappy) **Affected:** 17.0-26.1

CWE-125

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.iq80.snappy:snappy). OSV.dev confirms the advisory and the source is publicly available, so a patch may be feasible — this has not been confirmed and requires reviewing the diff between the affected and fixed versions.

## CVE-2026-35244 MEDIUM CVSS 5.2 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.24.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology...

**Product:** Oracle Hyperion **Component:** Lifecycle Management **Affected:** 11.2.24.0.000

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34321 MEDIUM CVSS 4.8 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.7.9, 8.0.8.7 and 8.1.2.5. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or...

**Product:** Oracle Financial Services Applications **Component:** User Interface **Affected:** 8.0.7.9, 8.0.8.7, 8.1.2.5

CWE-285

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2023-35116 MEDIUM CVSS 4.7 PATCH-FEASIBLE

jackson-databind through 2.15.2 allows attackers to cause a denial of service or other unspecified impact via a crafted object that uses cyclic dependencies. NOTE: the vendor's perspective is that this is not a valid vulnerability report, because the steps of constructing a cyclic data structure and trying to serialize it cannot be achieved by an external attacker.

**Product:** Oracle Analytics **Component:** Platform Security (jackson-databind) **Affected:** 8.2.0.0.0

CWE-770

---

## CVE-2025-41254 MEDIUM CVSS 4.3 PATCH-FEASIBLE

STOMP over WebSocket applications may be vulnerable to a security bypass that allows an attacker to send unauthorized messages. Affected Spring Products and VersionsSpring Framework: * 6.2.0 - 6.2.11 * 6.1.0 - 6.1.23 * 6.0.x - 6.0.29 * 5.3.0 - 5.3.45 * Older, unsupported versions are also affected. MitigationUsers of affected versions should upgrade to the corresponding fixed version. Affected version(s)Fix versionAvailability6.2.x6.2.12OSS6.1.x6.1.24 Commercial https://enterprise.spring.io/ 6.0.xN/A Out of support https://spring.io/projects/spring-framework#support...

**Product:** Oracle Financial Services Applications, Oracle Fusion Middleware

**Component:** Platform (Spring Framework) **Affected:** 8.0.7.9, 8.0.8.7, 8.1.2.5

CWE-352

**Why this status:** `open-source Maven` Promoted from QUEUED-FOR-REVIEW: this CVE affects an open-source Java library published on Maven Central (Maven packages: org.springframework:spring-websocket). OSV.dev confirms the advisory, which means the source is publicly available and a fix can be derived by diffing the affected and fixed versions.

---

## CVE-2024-31573 MEDIUM CVSS 4.0 PATCH-FEASIBLE

XMLUnit for Java before 2.10.0, in the default configuration, might allow code execution via an untrusted stylesheet (used for an XSLT transformation), because XSLT extension functions are enabled.

**Product:** Oracle Fusion Middleware **Component:** Fabric Layer (xmlunit) **Affected:** 12.2.1.4.0, 14.1.2.0.0

CWE-669

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: a reference URL points to a candidate upstream fix (commit tier): https://github.com/xmlunit/xmlunit/commit/b81d48b71dfd2868bdfc30a3e17ff973f32bc15b. A patch may be feasible — this has not been confirmed and requires reviewing the linked change.

## CVE-2026-22014 LOW CVSS 3.8 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Workflow and Business Events). Supported versions that are affected are 12.2.7-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle User Management accessible data as well as unauthorized read access to a subset of Oracle User Management accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality...

**Product:** Oracle E-Business Suite **Component:** Workflow and Business Events **Affected:** 12.2.7-12.2.15

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-22018 LOW CVSS 3.7 PATCH-FEASIBLE

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this...

**Product:** Oracle Java SE **Component:** Libraries

**Affected:** Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18, 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17

CWE-770

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: Red Hat published an advisory (RHSA-2026:11403) confirming a fix exists; the linked Bugzilla ticket (https://bugzilla.redhat.com/show_bug.cgi?id=2460041) traces to the upstream OpenJDK source patch ARMR can derive a rule from.

## CVE-2025-11143 LOW CVSS 3.7 NO-EXPLOIT-DISCLOSURE

The Jetty URI parser has some key differences to other common parsers when evaluating invalid or unusual URIs. Differential parsing of URIs in systems using multiple components may result in security by-pass. For example a component that enforces a black list may interpret the URIs differently from one that generates a response. At the very least, differential parsing may divulge implementation details.

**Product:** Oracle GoldenGate **Component:** Java Delivery (Eclipse Jetty) **Affected:** 21.3-21.21, 23.4-23.10

CWE-20

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## CVE-2026-34268 LOW CVSS 2.9 PATCH-FEASIBLE

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM for...

**Product:** Oracle Java SE **Component:** Security

**Affected:** Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18, 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17

CWE-200

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: Red Hat published an advisory (RHSA-2026:11403) confirming a fix exists; the linked Bugzilla ticket (https://bugzilla.redhat.com/show_bug.cgi?id=2460043) traces to the upstream OpenJDK source patch ARMR can derive a rule from.

---

## CVE-2026-22007 LOW CVSS 2.9 PATCH-FEASIBLE

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18 and 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM for...

**Product:** Oracle Java SE **Component:** Security

**Affected:** Oracle Java SE: 8u481, 8u481-b50, 8u481-perf, 11.0.30, 17.0.18, 21.0.10, 25.0.2, 26; Oracle GraalVM for JDK: 17.0.18, 21.0.10; Oracle GraalVM Enterprise Edition: 21.3.17

CWE-200

**Why this status:** `patch-hint` Promoted from QUEUED-FOR-REVIEW: Red Hat published an advisory (RHSA-2026:11403) confirming a fix exists; the linked Bugzilla ticket (https://bugzilla.redhat.com/show_bug.cgi?id=2460038) traces to the upstream OpenJDK source patch ARMR can derive a rule from.

---

## CVE-2026-34312 LOW CVSS 2.4 NO-EXPLOIT-DISCLOSURE

Vulnerability in the RDBMS component of Oracle Database Server. Supported versions that are affected are 19.3-19.30. Easily exploitable vulnerability allows high privileged attacker having Row Access Method privilege with network access via multiple protocols to compromise RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of RDBMS accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).

**Product:** Oracle Database Server **Component:** RDBMS **Affected:** 19.3-19.30

CWE-284

**Why this status:** `no-exploit-disclosure` Promoted from QUEUED-FOR-REVIEW: this CVE affects a known product but has no open-source fix path and no known public exploit or POC. The vulnerability is theoretical with no actionable remediation available.

## Out-of-Scope CVEs (136)

These CVEs from this Oracle CPU are not in scope for Waratek ARMR coverage — they affect non-Java upstream libraries, native/C code, or products outside ARMR's mitigation scope, so no Java-level mitigation applies and no rulepack entry is shipped for them.

| CVE | Severity | Product |
|---|---|---|
| CVE-2026-35251 | HIGH | Oracle Virtualization |
| CVE-2026-35250 | LOW | Oracle Virtualization |
| CVE-2026-35249 | LOW | Oracle Virtualization |
| CVE-2026-35248 | MEDIUM | Oracle Virtualization |
| CVE-2026-35247 | MEDIUM | Oracle Virtualization |
| CVE-2026-35246 | HIGH | Oracle Virtualization |
| CVE-2026-35245 | HIGH | Oracle Virtualization |
| CVE-2026-35242 | HIGH | Oracle Virtualization |
| CVE-2026-35241 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-35240 | MEDIUM | Oracle MySQL |
| CVE-2026-35239 | MEDIUM | Oracle MySQL |
| CVE-2026-35238 | MEDIUM | Oracle MySQL |
| CVE-2026-35237 | MEDIUM | Oracle MySQL |
| CVE-2026-35236 | MEDIUM | Oracle MySQL |
| CVE-2026-35235 | MEDIUM | Oracle MySQL |
| CVE-2026-35234 | MEDIUM | Oracle MySQL |
| CVE-2026-35231 | HIGH | Oracle Financial Services Applications |
| CVE-2026-35230 | HIGH | Oracle Virtualization |
| CVE-2026- | HIGH | Oracle Database Server |

| CVE | Severity | Product |
| --- | --- | --- |
| 35229 | | |
| CVE-2026-34324 | MEDIUM | Oracle Life Science Applications |
| CVE-2026-34323 | MEDIUM | Oracle Life Science Applications |
| CVE-2026-34320 | HIGH | Oracle Financial Services Applications |
| CVE-2026-34319 | MEDIUM | Oracle MySQL |
| CVE-2026-34318 | MEDIUM | Oracle MySQL |
| CVE-2026-34317 | MEDIUM | Oracle MySQL |
| CVE-2026-34308 | MEDIUM | Oracle MySQL |
| CVE-2026-34306 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-34304 | MEDIUM | Oracle MySQL |
| CVE-2026-34303 | MEDIUM | Oracle MySQL |
| CVE-2026-34302 | MEDIUM | Oracle E-Business Suite |
| CVE-2026-34301 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-34300 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-34299 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-34298 | MEDIUM | Oracle E-Business Suite |
| CVE-2026-34297 | HIGH | Oracle E-Business Suite |
| CVE-2026-34296 | MEDIUM | Oracle Supply Chain |
| CVE-2026-34295 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-34293 | MEDIUM | Oracle MySQL |
| CVE-2026-34291 | HIGH | Oracle Fusion Middleware |

| CVE | Severity | Product |
|---|---|---|
| CVE-2026-34281 | MEDIUM | Oracle Systems |
| CVE-2026-34280 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-34278 | MEDIUM | Oracle MySQL |
| CVE-2026-34276 | MEDIUM | Oracle MySQL |
| CVE-2026-34275 | CRITICAL | Oracle E-Business Suite |
| CVE-2026-34274 | MEDIUM | Oracle E-Business Suite |
| CVE-2026-34272 | MEDIUM | Oracle MySQL |
| CVE-2026-34271 | MEDIUM | Oracle MySQL |
| CVE-2026-34270 | MEDIUM | Oracle MySQL |
| CVE-2026-34267 | MEDIUM | Oracle MySQL |
| CVE-2026-34266 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-3288 | HIGH | Oracle Communications |
| CVE-2026-31790 | HIGH | Oracle Database Server |
| CVE-2026-27830 | HIGH | Oracle Analytics |
| CVE-2026-27727 | HIGH | Oracle Analytics |
| CVE-2026-27099 | HIGH | Oracle Communications |
| CVE-2026-26007 | HIGH | Oracle Communications, Oracle Database Server |
| CVE-2026-25990 | HIGH | Oracle Financial Services Applications |
| CVE-2026-25968 | HIGH | Oracle Communications |
| CVE-2026-25646 | HIGH | Oracle Communications, Oracle Fusion Middleware |
| CVE-2026-25210 | MEDIUM | Oracle Communications, Oracle Financial Services Applications, Oracle Fusion Middleware |

| CVE | Severity | Product |
|---|---|---|
| CVE-2026-23865 | MEDIUM | Oracle Java SE |
| CVE-2026-23490 | HIGH | Oracle Communications |
| CVE-2026-22801 | MEDIUM | Oracle Supply Chain |
| CVE-2026-22184 | MEDIUM | Oracle Fusion Middleware |
| CVE-2026-22019 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-22017 | MEDIUM | Oracle MySQL |
| CVE-2026-22015 | MEDIUM | Oracle MySQL |
| CVE-2026-22013 | MEDIUM | Oracle Java SE |
| CVE-2026-22011 | HIGH | Oracle E-Business Suite |
| CVE-2026-22009 | MEDIUM | Oracle MySQL |
| CVE-2026-22008 | LOW | Oracle Java SE |
| CVE-2026-22006 | MEDIUM | Oracle PeopleSoft |
| CVE-2026-22005 | MEDIUM | Oracle MySQL |
| CVE-2026-22004 | MEDIUM | Oracle MySQL |
| CVE-2026-22003 | MEDIUM | Oracle Java SE |
| CVE-2026-22002 | MEDIUM | Oracle MySQL |
| CVE-2026-22001 | LOW | Oracle MySQL |
| CVE-2026-21999 | MEDIUM | Oracle Database Server |
| CVE-2026-21998 | MEDIUM | Oracle MySQL |
| CVE-2026-21997 | HIGH | Oracle Life Science Applications |
| CVE-2026-21945 | HIGH | Oracle Communications |

| CVE | Severity | Product |
|---|---|---|
| CVE-2026-21637 | HIGH | Oracle Communications |
| CVE-2026-21441 | HIGH | Oracle Analytics, Oracle Communications |
| CVE-2026-20652 | HIGH | Oracle Java SE |
| CVE-2026-1642 | HIGH | Oracle Communications |
| CVE-2026-0861 | HIGH | Oracle Communications |
| CVE-2025-9900 | HIGH | Oracle Communications, Oracle Supply Chain |
| CVE-2025-9232 | MEDIUM | Oracle Autonomous Health Framework |
| CVE-2025-9230 | HIGH | Oracle Communications, Oracle JD Edwards |
| CVE-2025-9086 | HIGH | Oracle Communications, Oracle Hyperion |
| CVE-2025-8869 | MEDIUM | Oracle Siebel CRM |
| CVE-2025-8194 | HIGH | Oracle Communications, Oracle PeopleSoft |
| CVE-2025-6965 | HIGH | Oracle Communications |
| CVE-2025-69223 | HIGH | Oracle Communications, Oracle Siebel CRM |
| CVE-2025-68973 | HIGH | Oracle Communications |
| CVE-2025-68615 | CRITICAL | Oracle Communications, Oracle Fusion Middleware |
| CVE-2025-68431 | MEDIUM | Oracle Fusion Middleware |
| CVE-2025-68121 | CRITICAL | Oracle TimesTen In-Memory Database |
| CVE-2025-66418 | HIGH | Oracle Communications, Oracle Utilities Applications, Oracle PeopleSoft |
| CVE-2025-65082 | MEDIUM | Oracle Fusion Middleware |
| CVE-2025-65018 | HIGH | Oracle Hyperion |
| CVE-2025-61984 | LOW | Oracle Communications |

| CVE | Severity | Product |
|---|---|---|
| CVE-2025-61729 | HIGH | Oracle Blockchain Platform |
| CVE-2025-59775 | HIGH | Oracle Fusion Middleware |
| CVE-2025-59465 | HIGH | Oracle Blockchain Platform |
| CVE-2025-58754 | HIGH | Oracle PeopleSoft |
| CVE-2025-58181 | MEDIUM | Oracle Communications |
| CVE-2025-58098 | HIGH | Oracle Communications, Oracle Fusion Middleware |
| CVE-2025-58050 | MEDIUM | Oracle Communications |
| CVE-2025-55754 | CRITICAL | Oracle Communications |
| CVE-2025-55163 | HIGH | Oracle Communications, Oracle Financial Services Applications |
| CVE-2025-55130 | CRITICAL | Oracle Communications |
| CVE-2025-54571 | MEDIUM | Oracle Hyperion |
| CVE-2025-5372 | MEDIUM | Oracle Communications |
| CVE-2025-53643 | LOW | Oracle Utilities Applications |
| CVE-2025-5318 | HIGH | Oracle Communications, Oracle MySQL, Oracle Blockchain Platform |
| CVE-2025-52967 | MEDIUM | Oracle Communications |
| CVE-2025-43967 | LOW | Oracle PeopleSoft |
| CVE-2025-33042 | HIGH | Oracle Analytics, Oracle Communications, Oracle Fusion Middleware, Oracle GoldenGate |
| CVE-2025-32990 | MEDIUM | Oracle Communications |
| CVE-2025-31948 | MEDIUM | Oracle Database Server |
| CVE-2025-26791 | MEDIUM | Oracle Communications, Oracle Construction and Engineering |
| CVE-2025-26333 | MEDIUM | Oracle Communications, Oracle Enterprise Manager |

| CVE | Severity | Product |
| --- | --- | --- |
| CVE-2025-15467 | HIGH | Oracle Analytics, Oracle Communications, Oracle MySQL, Oracle PeopleSoft, Oracle Autonomous Health Framework |
| CVE-2025-15284 | MEDIUM | Oracle Communications |
| CVE-2025-14104 | MEDIUM | Oracle Communications |
| CVE-2025-14017 | MEDIUM | Oracle Communications, Oracle MySQL, Oracle PeopleSoft |
| CVE-2025-13601 | HIGH | Oracle Siebel CRM |
| CVE-2025-13151 | HIGH | Oracle Communications |
| CVE-2025-0725 | HIGH | Oracle Fusion Middleware |
| CVE-2024-6387 | HIGH | Oracle Systems |
| CVE-2024-56406 | HIGH | Oracle Commerce, Oracle Enterprise Manager |
| CVE-2024-5535 | CRITICAL | Oracle Communications |
| CVE-2024-45339 | HIGH | Oracle Communications |
| CVE-2024-43394 | HIGH | Oracle Fusion Middleware |
| CVE-2023-5388 | MEDIUM | Oracle JD Edwards |