Oracle Critical Patch Update January 2026: Waratek Coverage Report

Generated 05/06/2026, 14:35:03 · 2026-Q1 · Rulepack `vcpu-rulepack-2026-04-15-b75`

Oracle advisory: https://www.oracle.com/security-alerts/cpujan2026.html (https://www.oracle.com/security-alerts/cpujan2026.html)

Coverage Summary

158	51	51	1
CVEs in CPU	In scope for Java	Categorized	ARMR patches

By coverage mechanism

ARMR patch	1
ARMR secure-rule	10
No exploit disclosure	13
Patch feasible	27
Out of scope	107

By severity

CRITICAL	12
HIGH	62
MEDIUM	75
LOW	9

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 31 CVEs in this CPU	12 / 12 covered	· 11.4.0 · 15.0.0.0 · 15.0.0.0, 15.0.1.0 +17 more
Oracle Fusion Middleware 28 CVEs in this CPU	14 / 14 covered	· 11.4.0 · 12.2.1.4.0 · 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 +13 more
Oracle Financial Services Applications 16 CVEs in this CPU	11 / 11 covered	· 11.4.0 · 14.0.0.0.0-14.8.0.0.0 · 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0, 14.8.0.0.0 +11 more
Oracle MySQL 15 CVEs in this CPU	0 / 0 covered	· 11.4.0 · 7.6.0-7.6.36, 8.0.0-8.0.44, 8.4.0-8.4.7, 9.0.0-9.5.0 · 8.0.0-8.0.44, 8.4.0-8.4.7, 9.0.0-9.5.0 +3 more
Oracle Siebel CRM 14 CVEs in this CPU	7 / 7 covered	· 11.4.0 · 14.5.0.15.0, 14.6.0.11.0, 14.7.0.9.0, 14.8.0.1.0, 14.8.1.0.0 · 17.0-25.11 +5 more
Oracle Virtualization 14 CVEs in this CPU	0 / 0 covered	· 7.1.14, 7.2.4
Oracle PeopleSoft 12 CVEs in this CPU	5 / 5 covered	· 11.4.0 · 2.5.0.2.10, 2.6.0.1.9, 2.6.0.2.5 · 8.4.0-8.4.7 +3 more
Oracle Java SE 11 CVEs in this CPU	3 / 3 covered	· Oracle JDK Mission Control: 9.1.1 · Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17, 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16 · Oracle Java SE: 8u471-b50
Oracle Supply Chain 9 CVEs in this CPU	5 / 5 covered	· 21.1.0 · 23.4.0-23.26.0 · 6.2.4 +1 more
Oracle Analytics 8 CVEs in this CPU	5 / 5 covered	· 11.4.0 · 7.6.0.0.0, 8.2.0.0.0 · 7.6.0.0.0, 8.2.0.0.0, 12.2.1.4.0 +3 more

PRODUCT FAMILY	COVERAGE	AFFECTED VERSIONS
Oracle Construction and Engineering 7 CVEs in this CPU	6 / 6 covered	· 11.4.0 · 19.1.0.0.0-19.1.0.0.20, 21.3-21.20, 23.4-23.10 · 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.16, 24.12.0-24.12.12, 25.12.0 +3 more
Oracle Database Server 7 CVEs in this CPU	3 / 3 covered	· 19.3-19.29, 21.3-21.20 · 19.3-19.29, 23.4.0-23.26.0 · 21.3-21.20, 23.4.0-23.26.0 +1 more
Oracle JD Edwards 7 CVEs in this CPU	1 / 1 covered	· 16.0.3, 19.0.1 · 8.60, 8.61, 8.62 · 9.2.0.0-9.2.26.0 +1 more
Oracle Commerce 6 CVEs in this CPU	4 / 4 covered	· 11.4.0 · 24.4.4, 25.4.0
Oracle Hyperion 6 CVEs in this CPU	1 / 1 covered	· 11.4.0 · 12.2.1.4.0, 14.1.2.0.0 · 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0, 14.8.0.0.0 +2 more
Oracle Retail Applications 6 CVEs in this CPU	5 / 5 covered	· 11.4.0 · 16.0.3, 19.0.1 · 24.4.4, 25.4.0 +2 more
Oracle E-Business Suite 5 CVEs in this CPU	1 / 1 covered	· 12.2.3-12.2.15 · 9.3.6
Oracle GoldenGate 5 CVEs in this CPU	5 / 5 covered	· 11.4.0 · 19.1.0.0.0-19.1.0.0.11 · 19.1.0.0.0-19.1.0.0.20, 21.3-21.20, 23.4-23.10 +1 more
Oracle Health Sciences Applications 5 CVEs in this CPU	0 / 0 covered	· 7.0.1.0
Oracle Systems 5 CVEs in this CPU	0 / 0 covered	· 10, 11 · 11 · 8.8

PRODUCT FAMILY	COVERAGE	AFFECTED VERSIONS
Oracle Utilities Applications 5 CVEs in this CPU	4 / 4 covered	· 11.4.0 · 2.5.0.2.10, 2.6.0.1.9, 2.6.0.2.5 · 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0, 4.4.0.4.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.3, 4.5.0.2.0, 25.4, 25.10 +2 more
Oracle HealthCare Applications 4 CVEs in this CPU	4 / 4 covered	· 11.4.0 · 19.1.0.0.0-19.1.0.0.20, 21.3-21.20, 23.4-23.10 · 4.0.0
Oracle Hospitality Applications 4 CVEs in this CPU	4 / 4 covered	· 11.4.0 · 5.6.19, 5.6.25, 5.6.26, 5.6.27 · 9.3.6
Oracle Enterprise Manager 2 CVEs in this CPU	2 / 2 covered	· 11.4.0 · 24.1
Oracle APEX 1 CVE in this CPU	0 / 0 covered	· 23.2.0, 23.2.1, 24.1.0, 24.2.0, 24.2.1
Oracle Essbase 1 CVE in this CPU	1 / 1 covered	· 21.8.0.0.0
Oracle Graph Server and Client 1 CVE in this CPU	1 / 1 covered	· 24.4.4, 25.4.0
Oracle NoSQL Database 1 CVE in this CPU	1 / 1 covered	· 1.5, 1.6
Oracle Secure Backup 1 CVE in this CPU	0 / 0 covered	· 19.1.0.0.0-19.1.0.1.0
Oracle Zero Data Loss Recovery Appliance 1 CVE in this CPU	0 / 0 covered	· 23.1.0-23.1.202509

Changes Since Prior CPU

Comparing against **Oracle Critical Patch Update October 2025** (rulepack `vcpu-rulepack-2025-09-02-b44`)

121 new CVEs in this CPU advisory

CVE-2026-21990
CVE-2026-21989
CVE-2026-21988
CVE-2026-21987
CVE-2026-21986
CVE-2026-21985
CVE-2026-21984
CVE-2026-21983
CVE-2026-21982
CVE-2026-21981
CVE-2026-21980
CVE-2026-21979
CVE-2026-21978
CVE-2026-21977
CVE-2026-21976
CVE-2026-21975
CVE-2026-21974
CVE-2026-21973
CVE-2026-21972
CVE-2026-21971
CVE-2026-21970
CVE-2026-21969
CVE-2026-21968
CVE-2026-21967
CVE-2026-21966
CVE-2026-21965
CVE-2026-21964
CVE-2026-21963
CVE-2026-21962
CVE-2026-21961
CVE-2026-21960
CVE-2026-21959
CVE-2026-21957
CVE-2026-21956
CVE-2026-21955
CVE-2026-21952
CVE-2026-21951
CVE-2026-21950
CVE-2026-21949
CVE-2026-21948
CVE-2026-21947
CVE-2026-21946
CVE-2026-21945
CVE-2026-21944

CVE-2026-21943
CVE-2026-21942
CVE-2026-21941
CVE-2026-21940
CVE-2026-21939
CVE-2026-21938
CVE-2026-21937
CVE-2026-21936
CVE-2026-21935
CVE-2026-21934
CVE-2026-21933
CVE-2026-21932
CVE-2026-21931
CVE-2026-21930
CVE-2026-21929
CVE-2026-21928
CVE-2026-21927
CVE-2026-21926
CVE-2026-21925
CVE-2026-21924
CVE-2026-21923
CVE-2026-21922
CVE-2025-9900
CVE-2025-9230
CVE-2025-8194
CVE-2025-68161
CVE-2025-67735
CVE-2025-66566
CVE-2025-66516
CVE-2025-66418
CVE-2025-65082
CVE-2025-65018
CVE-2025-64718
CVE-2025-61795
CVE-2025-6052
CVE-2025-6021
CVE-2025-5987
CVE-2025-59419
CVE-2025-59250
CVE-2025-58098
CVE-2025-55039
CVE-2025-54988
CVE-2025-54874
CVE-2025-54571
CVE-2025-5372
CVE-2025-50059

CVE-2025-49844
CVE-2025-48060
CVE-2025-47219
CVE-2025-46727
CVE-2025-43967
CVE-2025-43368
CVE-2025-41248
CVE-2025-32988
CVE-2025-30065
CVE-2025-26791
CVE-2025-26333
CVE-2025-23048
CVE-2025-22228
CVE-2025-12383
CVE-2025-12183
CVE-2024-56406
CVE-2024-47252
CVE-2024-46901
CVE-2024-43796
CVE-2024-43204
CVE-2024-42516
CVE-2023-42670
CVE-2023-29081
CVE-2023-1393
CVE-2022-45047
CVE-2022-41342
CVE-2022-23395
CVE-2021-45105
CVE-2021-43113
CVE-2021-33813
CVE-2021-23926

3 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.

2022vcpu.armr

MODIFIED CVE-2022-34169

2021vcpu.armr

MODIFIED CVE-2021-2432

2018vcpu.armr

MODIFIED CVE-2018-2938

Per-CVE Coverage

CVE-2025-30065 CRITICAL CVSS 10.0 MITIGATED-BY-SECURE-RULE

Schema parsing in the parquet-avro module of Apache Parquet 1.15.0 and previous versions allows bad actors to execute arbitrary code Users are recommended to upgrade to version 1.15.1, which fixes the issue.

Product: Oracle NoSQL Database **Component:** Administration (Apache Parquet Java) **Affected:** 1.5, 1.6

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-2024-52046 CRITICAL CVSS 10.0 MITIGATED-BY-SECURE-RULE

The ObjectSerializationDecoder in Apache MINA uses Java's native deserialization protocol to process incoming serialized data but lacks the necessary security checks and defenses. This vulnerability allows attackers to exploit the deserialization process by sending specially crafted malicious serialized data, potentially leading to remote code execution (RCE) attacks. This issue affects MINA core versions 2.0.X, 2.1.X and 2.2.X, and will be fixed by the releases 2.0.27, 2.1.10 and 2.2.4. It's also important to note that an application using MINA core...

Product: Oracle HealthCare Applications **Component:** XAD-PID Change Management XPID (Apache Mina)

Affected: 4.0.0

CWE-502 CWE-94

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-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 Analytics **Component:** Core (Apache Mina SSHD) **Affected:** 8.2.0.0.0

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-2021-43113 CRITICAL CVSS 9.8 MITIGATED-BY-SECURE-RULE

iTextPDF in iText 7 and up to (excluding 4.4.13.3) 7.1.17 allows command injection via a CompareTool filename that is mishandled on the gs (aka Ghostscript) command line in GhostscriptHelper.java.

Product: Oracle Construction and Engineering **Component:** Reports (iTextPDF)

Affected: 21.12.0-21.12.17, 22.12.0-22.12.15, 23.12.0-23.12.16, 24.12.0-24.12.12, 25.12.0

CWE-77

Why this status: `secure-rule-match` Promoted to MITIGATED-BY-SECURE-RULE: this CVE's weakness (CWE-77: 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-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 Database Server, Oracle Fusion Middleware **Component:** Fleet Patching and Provisioning (Eclipse Jersey)

Affected: 23.4.0-23.26.0

CWE-362 CWE-296

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-2021-23926 CRITICAL CVSS 9.1 MITIGATED-BY-SECURE-RULE

The XML parsers used by XMLBeans up to version 2.6.0 did not set the properties needed to protect the user from malicious XML input. Vulnerabilities include possibilities for XML Entity Expansion attacks. Affects XMLBeans up to and including v2.6.0.

Product: Oracle Analytics **Component:** Core (Apache XMLBeans) **Affected:** 8.2.0.0.0

CWE-776

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 Supply Chain, Oracle Construction and Engineering, Oracle Retail Applications, Oracle E-Business Suite, Oracle Financial Services Applications, Oracle Communications

Component: Security (Apache Commons BeanUtils) **Affected:** 9.3.6

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 Java SE **Component:** Mission Control (lz4-java) **Affected:** Oracle JDK Mission Control: 9.1.1

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: 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 Analytics **Component:** Analytics Server (jackson-core) **Affected:** 7.6.0.0.0, 8.2.0.0.0

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-2026-21967 HIGH CVSS 8.6 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Hospitality OPERA 5 product of Oracle Hospitality Applications (component: Opera Servlet). Supported versions that are affected are 5.6.19.23, 5.6.25.17, 5.6.26.10 and 5.6.27.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality OPERA…

Product: Oracle Hospitality Applications **Component:** Opera Servlet **Affected:** 5.6.19, 5.6.25, 5.6.26, 5.6.27

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-2025-66516 HIGH CVSS 8.4 MITIGATED-BY-SECURE-RULE

Critical XXE in Apache Tika tika-core (1.13-3.2.1), tika-pdf-module (2.0.0-3.2.1) and tika-parsers (1.13-1.28.5) modules on all platforms allows an attacker to carry out XML External Entity injection via a crafted XFA file inside of a PDF. This CVE covers the same vulnerability as in CVE-2025-54988. However, this CVE expands the scope of affected packages in two ways. First, while the entrypoint for the vulnerability was the tika-parser-pdf-module as reported in CVE-2025-54988, the vulnerability and its fix were in tika-core. Users who upgraded the tika-parser-pdf-module but did not...

Product: Oracle Commerce, Oracle Construction and Engineering, Oracle PeopleSoft, Oracle Communications, Oracle Fusion Middleware

Component: Workbench (Apache Tika) **Affected:** 11.4.0

CWE-611

CVE-2025-54988 HIGH CVSS 8.4 MITIGATED-BY-SECURE-RULE

Critical XXE in Apache Tika (tika-parser-pdf-module) in Apache Tika 1.13 through and including 3.2.1 on all platforms allows an attacker to carry out XML External Entity injection via a crafted XFA file inside of a PDF. An attacker may be able to read sensitive data or trigger malicious requests to internal resources or third-party servers. Note that the tika-parser-pdf-module is used as a dependency in several Tika packages including at least: tika-parsers-standard-modules, tika-parsers-standard-package, tika-app, tika-grpc and tika-server-standard. Users are recommended to upgrade to...

Product: Oracle Fusion Middleware **Component:** Oracle Business Rules (Apache Commons Compress)

Affected: 14.1.2.0.0

CWE-611

Why this status: `secure-rule-match` Promoted to MITIGATED-BY-SECURE-RULE: this CVE's weakness (CWE-611: XML External Entity Reference) can be mitigated by an ARMR xxe security rule that blocks this class of attack at the JVM level, without requiring a CVE-specific patch.

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 Essbase **Component:** Essbase Web Platform (lz4-java) **Affected:** 21.8.0.0.0

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-2025-59250 HIGH CVSS 8.1 PATCH-FEASIBLE

Improper input validation in JDBC Driver for SQL Server allows an unauthorized attacker to perform spoofing over a network.

Product: Oracle GoldenGate **Component:** Java Delivery (JDBC Driver for SQL Server) **Affected:** 21.3-21.20, 23.4-23.10

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: com.microsoft.sqlserver:mssql-jdbc). 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-2025-5115 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 Supply Chain, Oracle Financial Services Applications, Oracle Communications, Oracle Fusion Middleware

Component: Internal Operations (Eclipse Jetty) **Affected:** 21.1.0

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-2025-48989 HIGH CVSS 7.5 PATCH-FEASIBLE

Improper Resource Shutdown or Release vulnerability in Apache Tomcat made Tomcat vulnerable to the made you reset attack. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.9, from 10.1.0-M1 through 10.1.43 and from 9.0.0.M1 through 9.0.107. Older, EOL versions may also be affected. Users are recommended to upgrade to one of versions 11.0.10, 10.1.44 or 9.0.108 which fix the issue.

Product: Oracle Supply Chain, Oracle Utilities Applications, Oracle Siebel CRM **Component:** Security (Apache Tomcat)

Affected: 9.3.6

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-coyote, 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-2025-48976 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 Supply Chain, Oracle Hospitality Applications, Oracle Financial Services Applications, Oracle Siebel CRM, Oracle Communications, Oracle Fusion Middleware

Component: Folders, Files and Attachments (Apache Commons FileUpload) **Affected:** 9.3.6

CWE-770

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 Commerce, Oracle Construction and Engineering, Oracle Retail Applications, Oracle HealthCare Applications, Oracle Financial Services Applications, Oracle Communications, Oracle Fusion Middleware

Component: Content Acquisition System, Workbench, Endeca Application Controller (Spring Framework) **Affected:** 11.4.0

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 Financial Services Applications, Oracle Fusion Middleware **Component:** Installer (Spring Security)

Affected: 8.1.3.2

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-2025-27817 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:** Accessibility (Apache Kafka)

Affected: 14.5.0.15.0, 14.6.0.11.0, 14.7.0.9.0, 14.8.0.1.0, 14.8.1.0.0

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-2021-33813 HIGH CVSS 7.5 MITIGATED-BY-SECURE-RULE

An XXE issue in SAXBuilder in JDOM through 2.0.6 allows attackers to cause a denial of service via a crafted HTTP request.

Product: Oracle Siebel CRM **Component:** Application Interface (JDOM) **Affected:** 17.0-25.11

CWE-611

CVE-2025-22228 HIGH CVSS 7.4 PATCH-FEASIBLE

BCryptPasswordEncoder.matches(CharSequence,String) will incorrectly return true for passwords larger than 72 characters as long as the first 72 characters are the same.

Product: Oracle Financial Services Applications **Component:** Common Core (Spring Security) **Affected:** 14.5.0.14.0

CWE-287 CWE-521

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-crypto). 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-2024-13009 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 Enterprise Manager, Oracle Fusion Middleware **Component:** Gateway (Eclipse Jetty) **Affected:** 24.1

CWE-404

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 Database Server **Component:** SQLcl **Affected:** 23.4.0-23.26.0

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 Communications **Component:** Security (Netty) **Affected:** 25.1.0

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-2025-27533 MEDIUM CVSS 6.9 PATCH-FEASIBLE

Memory Allocation with Excessive Size Value vulnerability in Apache ActiveMQ. During unmarshalling of OpenWire commands the size value of buffers was not properly validated which could lead to excessive memory allocation and be exploited to cause a denial of service (DoS) by depleting process memory, thereby affecting applications and services that rely on the availability of the ActiveMQ broker when not using mutual TLS connections. This issue affects Apache ActiveMQ: from 6.0.0 before 6.1.6, from 5.18.0 before 5.18.7, from 5.17.0 before 5.17.7, before 5.16.8. ActiveMQ 5.19.0 is not...

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

CWE-789

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.activemq:activemq-openwire-legacy, org.apache.activemq:activemq-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-2025-4949 MEDIUM CVSS 6.8 MITIGATED-BY-SECURE-RULE

In Eclipse JGit versions 7.2.0.202503040940-r and older, the ManifestParser class used by the repo command and the AmazonS3 class used to implement the experimental amazons3 git transport protocol allowing to store git pack files in an Amazon S3 bucket, are vulnerable to XML External Entity (XXE) attacks when parsing XML files. This vulnerability can lead to information disclosure, denial of service, and other security issues.

Product: Oracle Fusion Middleware **Component:** Security (Eclipse JGit) **Affected:** 14.1.2.0.0

CWE-611 CWE-827

Why this status: `secure-rule-match` Promoted to MITIGATED-BY-SECURE-RULE: this CVE's weakness (CWE-611: XML External Entity Reference) can be mitigated by an ARMR xxe security rule that blocks this class of attack at the JVM level, without requiring a CVE-specific patch.

CVE-2026-21978 MEDIUM CVSS 6.5 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Relationship Pricing). Supported versions that are affected are 14.0.0.0.0-14.8.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector:...

Product: Oracle Financial Services Applications **Component:** Relationship Pricing **Affected:** 14.0.0.0.0-14.8.0.0.0

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-2025-67735 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 Database Server **Component:** Oracle Graal Development Kit for Micronaut (Nimbus JOSE+JWT)

Affected: 19.3-19.29, 23.4.0-23.26.0

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-2025-55039 MEDIUM CVSS 6.5 PATCH-FEASIBLE

This issue affects Apache Spark versions before 3.4.4, 3.5.2 and 4.0.0. Apache Spark versions before 4.0.0, 3.5.2 and 3.4.4 use an insecure default network encryption cipher for RPC communication between nodes. When spark.network.crypto.enabled is set to true (it is set to false by default), but spark.network.crypto.cipher is not explicitly configured, Spark defaults to AES in CTR mode (AES/CTR/NoPadding), which provides encryption without authentication. This vulnerability allows a man-in-the-middle attacker to modify encrypted RPC traffic undetected by flipping bits in ciphertext,...

Product: Oracle GoldenGate **Component:** General (Apache Spark) **Affected:** 19.1.0.0.0-19.1.0.0.11

CWE-326 CWE-347

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.spark:spark-network-common_2.13, org.apache.spark:spark-network-common_2.12). 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-2025-8916 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 Utilities Applications, Oracle Siebel CRM, Oracle Communications

Component: Security (Bouncy Castle Java Library)

Affected: 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0, 4.4.0.4.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.3, 4.5.0.2.0, 25.4, 25.10

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 GoldenGate, Oracle Construction and Engineering, Oracle HealthCare Applications, Oracle Communications

Component: Third Party (Apache Log4j) **Affected:** 19.1.0.0.0-19.1.0.0.20, 21.3-21.20, 23.4-23.10

CWE-297 CWE-295

CVE-2026-21966 MEDIUM CVSS 6.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera). Supported versions that are affected are 5.6.19.23, 5.6.25.17, 5.6.26.10 and 5.6.27.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality OPERA 5 Property Services, attacks may significantly impact additional products (scope...

Product: Oracle Hospitality Applications **Component:** Opera **Affected:** 5.6.19, 5.6.25, 5.6.26, 5.6.27

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-2026-21951 MEDIUM CVSS 6.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Integration Broker). Supported versions that are affected are 8.60, 8.61 and 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...

Product: Oracle PeopleSoft **Component:** Integration Broker **Affected:** 8.60, 8.61, 8.62

CWE-79

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-2026-21946 MEDIUM CVSS 6.1 NO-EXPLOIT-DISCLOSURE

Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.0.0-9.2.26.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized...

Product: Oracle JD Edwards **Component:** Web Runtime SEC **Affected:** 9.2.0.0-9.2.26.0

CWE-79

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-2026-21938 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 8.60, 8.61 and 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...

Product: Oracle PeopleSoft **Component:** Portal **Affected:** 8.60, 8.61, 8.62

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-2026-21933 MEDIUM CVSS 6.1 NO-EXPLOIT-DISCLOSURE

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: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. 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 require human interaction...

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

Affected: Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17, 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16

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-2022-23395 MEDIUM CVSS 6.1 NO-EXPLOIT-DISCLOSURE

jQuery Cookie 1.4.1 is affected by prototype pollution, which can lead to DOM cross-site scripting (XSS).

Product: Oracle Siebel CRM **Component:** Application Interface (jquery-cookie) **Affected:** 17.0-25.9

CWE-1321

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 **Component:** Security (Jakarta Mail) **Affected:** 25.0.1

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, com.sun.mail:jakarta.mail). 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-2021-45105 MEDIUM CVSS 5.9 MITIGATED-BY-PATCH-RULE

Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.

Product: Oracle Fusion Middleware **Component:** Core (Apache Log4j) **Affected:** 12.2.1.4.0

CWE-20 CWE-674

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

ARMR:CVE-2021-45105.armr (https://github.com/waratek/java-patches/blob/develop/rules/libraries/apache/log4j/CVE-2021-45105/patch/2.6/CVE-2021-45105.armr) (spec 2.6)

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:** Centralized Third Party Jars (Nimbus JOSE+JWT)

Affected: 12.2.1.4.0, 14.1.1.0.0, 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 Construction and Engineering, Oracle Financial Services Applications

Component: Integrators (Apache CXF) **Affected:** 22.12.0.0-22.12.20.0, 23.12.0.0-23.12.17.0, 24.12.0.0-24.12.11.0

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.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-2025-59419 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 GoldenGate **Component:** Java Delivery (Netty) **Affected:** 21.3-21.20, 23.4-23.10

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-2025-25193 MEDIUM CVSS 5.5 PATCH-FEASIBLE

Netty, an asynchronous, event-driven network application framework, has a vulnerability in versions up to and including 4.1.118.Final. An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crash. A similar issue was previously reported as CVE-2024-47535. This issue was fixed, but the fix was incomplete in that null-bytes were not counted against the input limit. Commit...

Product: Oracle Communications **Component:** Security (Netty) **Affected:** 15.0.0.0, 15.0.1.0

CWE-400

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/d1fbda62d3a47835d3fb35db8bd42ecc205a5386. ARMR can derive a patch from the linked commit.

CVE-2026-21934 MEDIUM CVSS 5.4 NO-EXPLOIT-DISCLOSURE

Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Push Notifications). Supported versions that are affected are 8.60, 8.61 and 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 update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1...

Product: Oracle PeopleSoft **Component:** Push Notifications **Affected:** 8.60, 8.61, 8.62

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-2026-21924 MEDIUM CVSS 5.4 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Utilities Application Framework product of Oracle Utilities Applications (component: General). Supported versions that are affected are 4.4.0.3.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.3, 4.5.0.2.0, 25.4 and 25.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Utilities Application Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Utilities Application Framework, attacks may significantly impact additional products...

Product: Oracle Utilities Applications **Component:** General

Affected: 4.4.0.3.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.3, 4.5.0.2.0, 25.4, 25.10

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-2025-61795 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 Graph Server and Client, Oracle Commerce, Oracle Retail Applications, Oracle Financial Services Applications, Oracle Communications

Component: Packaging (Apache Tomcat) **Affected:** 24.4.4, 25.4.0

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 Commerce, Oracle Utilities Applications, Oracle Analytics, Oracle Hospitality Applications, Oracle GoldenGate, Oracle Retail Applications, Oracle Enterprise Manager, Oracle PeopleSoft, Oracle Financial Services Applications, Oracle Siebel CRM, Oracle Communications, Oracle Fusion Middleware, Oracle Hyperion

Component: Dynamo Application Framework (Apache Commons Lang) **Affected:** 11.4.0

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 Supply Chain, Oracle Analytics, Oracle Fusion Middleware

Component: Document Management (Apache POI) **Affected:** 9.3.6

CWE-20

CVE-2026-21925 MEDIUM CVSS 4.8 NO-EXPLOIT-DISCLOSURE

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: RMI). Supported versions that are affected are Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17 and 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16. 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 vulnerability can...

Product: Oracle Java SE **Component:** RMI

Affected: Oracle Java SE: 8u471, 8u471-b50, 8u471-perf, 11.0.29, 17.0.17, 21.0.9, 25.0.1; Oracle GraalVM for JDK: 17.0.17, 21.0.9; Oracle GraalVM Enterprise Edition: 21.3.16

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-2024-47554 MEDIUM CVSS 4.3 NO-EXPLOIT-DISCLOSURE

Uncontrolled Resource Consumption vulnerability in Apache Commons IO. The org.apache.commons.io.input.XmlStreamReader class may excessively consume CPU resources when processing maliciously crafted input. This issue affects Apache Commons IO: from 2.0 before 2.14.0. Users are recommended to upgrade to version 2.14.0 or later, which fixes the issue.

Product: Oracle HealthCare Applications, Oracle Fusion Middleware **Component:** Install (Apache Commons IO)

Affected: 4.0.0

CWE-400

Out-of-Scope CVEs (107)

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-2026-21990	HIGH	Oracle Virtualization
CVE-2026-21989	HIGH	Oracle Virtualization
CVE-2026-21988	HIGH	Oracle Virtualization
CVE-2026-21987	HIGH	Oracle Virtualization
CVE-2026-21986	HIGH	Oracle Virtualization
CVE-2026-21985	MEDIUM	Oracle Virtualization
CVE-2026-21984	HIGH	Oracle Virtualization
CVE-2026-21983	HIGH	Oracle Virtualization
CVE-2026-21982	HIGH	Oracle Virtualization
CVE-2026-21981	MEDIUM	Oracle Virtualization
CVE-2026-21980	MEDIUM	Oracle Health Sciences Applications
CVE-2026-21979	MEDIUM	Oracle Hyperion
CVE-2026-21977	LOW	Oracle Zero Data Loss Recovery Appliance
CVE-2026-21976	HIGH	Oracle Analytics
CVE-2026-21975	MEDIUM	Oracle Database Server
CVE-2026-21974	MEDIUM	Oracle Health Sciences Applications
CVE-2026-21973	HIGH	Oracle Financial Services Applications
CVE-2026-21972	MEDIUM	Oracle E-Business Suite
CVE-2026-21971	MEDIUM	Oracle PeopleSoft
CVE-2026-21970	MEDIUM	Oracle Health Sciences Applications

CVE	Severity	Product
CVE-2026-21969	CRITICAL	Oracle Supply Chain
CVE-2026-21968	MEDIUM	Oracle MySQL
CVE-2026-21965	LOW	Oracle MySQL
CVE-2026-21964	MEDIUM	Oracle MySQL
CVE-2026-21963	MEDIUM	Oracle Virtualization
CVE-2026-21962	CRITICAL	Oracle Fusion Middleware
CVE-2026-21961	MEDIUM	Oracle PeopleSoft
CVE-2026-21960	MEDIUM	Oracle E-Business Suite
CVE-2026-21959	MEDIUM	Oracle E-Business Suite
CVE-2026-21957	HIGH	Oracle Virtualization
CVE-2026-21956	HIGH	Oracle Virtualization
CVE-2026-21955	HIGH	Oracle Virtualization
CVE-2026-21952	MEDIUM	Oracle MySQL
CVE-2026-21950	MEDIUM	Oracle MySQL
CVE-2026-21949	MEDIUM	Oracle MySQL
CVE-2026-21948	MEDIUM	Oracle MySQL
CVE-2026-21947	LOW	Oracle Java SE
CVE-2026-21945	HIGH	Oracle Java SE
CVE-2026-21944	MEDIUM	Oracle Supply Chain
CVE-2026-21943	MEDIUM	Oracle E-Business Suite

CVE	Severity	Product
CVE-2026-21942	MEDIUM	Oracle Systems
CVE-2026-21941	MEDIUM	Oracle MySQL
CVE-2026-21940	HIGH	Oracle Supply Chain
CVE-2026-21937	MEDIUM	Oracle MySQL
CVE-2026-21936	MEDIUM	Oracle MySQL
CVE-2026-21935	MEDIUM	Oracle Systems
CVE-2026-21932	HIGH	Oracle Java SE
CVE-2026-21931	MEDIUM	Oracle APEX
CVE-2026-21930	LOW	Oracle Systems
CVE-2026-21929	MEDIUM	Oracle MySQL
CVE-2026-21928	MEDIUM	Oracle Systems
CVE-2026-21927	MEDIUM	Oracle Systems
CVE-2026-21926	HIGH	Oracle Siebel CRM
CVE-2026-21923	MEDIUM	Oracle Health Sciences Applications
CVE-2026-21922	MEDIUM	Oracle Hyperion
CVE-2025-9900	HIGH	Oracle Communications
CVE-2025-9230	HIGH	Oracle MySQL, Oracle Analytics, Oracle PeopleSoft, Oracle Financial Services Applications
CVE-2025-9086	HIGH	Oracle Commerce, Oracle MySQL, Oracle PeopleSoft
CVE-2025-8194	HIGH	Oracle Database Server, Oracle Communications
CVE-2025-7425	HIGH	Oracle Java SE

CVE	Severity	Product
CVE-2025-6965	HIGH	Oracle MySQL, Oracle PeopleSoft, Oracle Siebel CRM
CVE-2025-66418	HIGH	Oracle Financial Services Applications, Oracle Communications
CVE-2025-65082	MEDIUM	Oracle Secure Backup
CVE-2025-65018	HIGH	Oracle MySQL, Oracle Communications
CVE-2025-64718	MEDIUM	Oracle Communications
CVE-2025-61755	LOW	Oracle Database Server
CVE-2025-6052	LOW	Oracle Java SE
CVE-2025-6021	HIGH	Oracle Java SE
CVE-2025-5987	HIGH	Oracle Communications
CVE-2025-59375	HIGH	Oracle Communications, Oracle Fusion Middleware
CVE-2025-58098	HIGH	Oracle Communications
CVE-2025-55163	HIGH	Oracle Utilities Applications, Oracle PeopleSoft, Oracle Financial Services Applications, Oracle Communications, Oracle Fusion Middleware
CVE-2025-54874	MEDIUM	Oracle Database Server, Oracle Supply Chain, Oracle Fusion Middleware
CVE-2025-54571	MEDIUM	Oracle Communications, Oracle Fusion Middleware
CVE-2025-5372	MEDIUM	Oracle Siebel CRM
CVE-2025-53643	LOW	Oracle Siebel CRM
CVE-2025-53547	HIGH	Oracle Siebel CRM
CVE-2025-5318	HIGH	Oracle Communications
CVE-2025-50059	HIGH	Oracle Commerce
CVE-2025-49844	CRITICAL	Oracle Communications

CVE	Severity	Product
CVE-2025-49796	CRITICAL	Oracle Financial Services Applications, Oracle Fusion Middleware, Oracle Hyperion
CVE-2025-48060	HIGH	Oracle Communications
CVE-2025-47219	HIGH	Oracle Java SE
CVE-2025-46727	HIGH	Oracle Communications
CVE-2025-4575	MEDIUM	Oracle Siebel CRM
CVE-2025-43967	LOW	Oracle Fusion Middleware, Oracle Hyperion
CVE-2025-43368	MEDIUM	Oracle Java SE
CVE-2025-32990	MEDIUM	Oracle Communications
CVE-2025-32988	MEDIUM	Oracle Communications
CVE-2025-27363	HIGH	Oracle JD Edwards, Oracle Hyperion
CVE-2025-27210	HIGH	Oracle PeopleSoft, Oracle JD Edwards
CVE-2025-26791	MEDIUM	Oracle Construction and Engineering
CVE-2025-26333	MEDIUM	Oracle Retail Applications, Oracle JD Edwards, Oracle Communications, Oracle Fusion Middleware
CVE-2025-23048	CRITICAL	Oracle Fusion Middleware
CVE-2024-57699	HIGH	Oracle Analytics
CVE-2024-56406	HIGH	Oracle Fusion Middleware
CVE-2024-47252	HIGH	Oracle Fusion Middleware
CVE-2024-46901	LOW	Oracle Communications
CVE-2024-43796	MEDIUM	Oracle JD Edwards
CVE-2024-43204	HIGH	Oracle Fusion Middleware

CVE	Severity	Product
CVE-2024-42516	HIGH	Oracle Fusion Middleware
CVE-2024-23807	CRITICAL	Oracle Siebel CRM
CVE-2024-12133	MEDIUM	Oracle Communications
CVE-2023-42670	MEDIUM	Oracle JD Edwards
CVE-2023-29081	MEDIUM	Oracle Health Sciences Applications
CVE-2023-1393	HIGH	Oracle JD Edwards
CVE-2022-41342	MEDIUM	Oracle Fusion Middleware

Report generated on 05/06/2026, 14:35:03. Rulepack tag: `vcpu-rulepack-2026-04-15-b75`.