Security Bulletin

SecB0013: CVE-2024-21147

Summary

First published: July 14, 2025

Description	CVE-2024-21147 is a high-severity vulnerability (CVSS 7.4) affecting the Java HotSpot Virtual Machine in Oracle Java and compatible distributions such as Amazon Corretto. This vulnerability may allow remote attackers to compromise Java-based applications under specific conditions involving unsafe deserialization or malformed input handling.
Products	enteliWEB (not affected)
Recommended Action	None. While enteliWEB is not affected, we take security seriously. The Amazon Corretto JDK will be **upgraded to version 21.0.4 or later** as part of the **enteliWEB 4.31 release**, eliminating any theoretical exposure and aligning with security best practices.

CVE ID	CVSS Vector	Score
CVE-2024-21147	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N	7.4

Security Bulletin

Description

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. 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.

Why enteliWEB Is Not Affected

- **JVM Isolation**
  enteliWEB's architecture does **not expose the Java Virtual Machine (JVM)** directly to end users. All interactions with Java components are mediated through internal logic and web services, preventing direct exploitation paths.
- **Controlled Use of Corretto 21.0.2**
  The affected module—Amazon Corretto 21.0.2—is used **exclusively within the BIRT Reporting Engine**, a subsystem of enteliWEB responsible for generating structured reports. This component is not exposed directly to users or external interfaces.
- **Sanitized and Internal Data Only**
  enteliWEB **does not provide any feature or interface** that allows customers to upload or submit XML, JSON, or serialized Java objects that could interact with the JVM. Report parameters are passed through the **PHP backend**, where they are **strictly sanitized** before being handed to the BIRT engine.

In one scenario, BIRT uses these sanitized parameters to issue SQL queries directly to the PostgreSQL server. In another, the PHP backend performs the database queries and passes only the result set to BIRT for rendering.

In both cases, **there is no possibility for interactive XML/JSON or raw serialized data from users to reach the JVM**. This architectural model inherently prevents exploitation of CVE-2024-21147.

Planned Remediation via Upgrade

While enteliWEB is not affected, we take security seriously. The Amazon Corretto JDK will be **upgraded to version 21.0.4 or later** as part of the **enteliWEB 4.31 release**, eliminating any theoretical exposure and aligning with security best practices.