Snyk Top 10: Java OSS Vulnerabilities 2022

These are the most prevalent **critical** and **high** open source vulnerabilities found by Snyk scans of Java apps in 2022.

01 Denial of Service (DoS)

Denial of service (DoS) describes a family of attacks, all aimed at making a system inaccessible to its intended and legitimate users. Attackers will attempt to trigger system crashes or spike resources to make services inoperable.

Top vuln: CVE-2020-36518
Fix: Upgrade `com.fasterxml.jackson.core:jackson-databind` to version 2.12.6.1, 2.13.2.1 or higher.

02 Deserialization of Untrusted Data

This is when an application deserializes untrusted data without sufficiently verifying that the resulting data will be valid, thus allowing the attacker to control the state or the flow of the execution.

Top vuln: CVE-2022-20190
Fix: Upgrade `com.fasterxml.jackson.core:jackson-databind` to version 2.9.10.7 or higher.

03 Remote Code Execution (RCE)

Remote code execution (RCE) allows an attacker to execute arbitrary code on a remote device. This is often done through injection attacks. In 2022, the big RCE vulnerability was Spring4Shell.

Top vuln: CVE-2022-22965
Fix: There is no fixed version for `Debian:9 libspring-java`.

04 Arbitrary Code Execution (ACE)

Arbitrary code execution (ACE) happens when an attacker is able to run commands or execute code of their choice on a target machine. If this code is executed over a network, it is sometimes referred to as remote code execution.

Top vuln: CVE-2022-42889
Fix: Upgrade `org.apache.commons:commons-text` to version 1.10.0 or higher.

05 SQL Injection

SQL injection is a common method used by attackers to manipulate and access database information. This is done by exploiting application vulnerabilities to inject malicious SQL code that alters SQL queries.

Top vuln: CVE-2022-23305
Fix: There is no fixed version for `log4j:log4j`.

06 Information Exposure

This is a type of broken access control vulnerability in which a user or attacker gains access to information that they are not explicitly authorized to view, including PII, company data, system data/metadata, and more.

Top vuln: Unassigned CWE-200
Fix: Upgrade `com.squareup.okhttp3:okhttp` to version 4.9.2 or higher.

07 Insecure Temporary File

An insecure temporary file is a file that is created by an application for temporary use, but is not properly secured. This can potentially create a security vulnerability by allowing attackers to access or modify the temporary file.

Top vuln: CVE-2022-27772
Fix: Upgrade `org.springframework.boot:spring-boot` to version 2.2.11.RELEASE or higher.

08 Authorization Bypass

This is when an attacker gains access to a system or data without proper authorization. They are able to obtain the privileges of an authorized user without having to authenticate.

Top vuln: CVE-2022-22978
Fix: Upgrade `org.springframework.security:spring-security-web` to version 5.5.7, 5.6.4 or higher.

09 Improper Resource Shutdown or Release

Improper resource shutdown or release is when the program does not release or incorrectly releases a resource before it is made available for reuse. This can lead to improper error handling, insufficient resource tracking, and also resource exhaustion.

Top vuln: CVE-2022-2191
Fix: Upgrade `org.eclipse.jetty:jetty-io` to version 10.0.10, 11.0.10 or higher.

10 XML External Entity (XXE) Injection

XXE Injection is a type of attack against an application that parses XML input. Attacks can include disclosing local files, which may contain sensitive data such as passwords or private user data, using file: schemes or relative paths in the system identifier.

Top vuln: CVE-2021-23926
Fix: Upgrade `org.apache.xmlbeans:xmlbeans` to version 3.0.0 or higher.