How to Read the S-BOM Scanning Report

The S-BOM scanning report is generated based on the Software Bill of Materials (S-BOM) file submitted with the APK, combined with data from the public CVE (Common Vulnerabilities and Exposures) database. The report highlights only **HIGH** and **CRITICAL** severity vulnerabilities to help submitters identify and address potential security risks by upgrading affected dependencies.

Report Structure

The report consists of two main sections:

1. Vulnerability Summary Table

This table lists components identified as potentially vulnerable.

- **Library**: Name of the affected component.
- **Vulnerability**: Reference to the public CVE ID.
- **Severity**: Severity level as classified by the CVE Program.
- **Status**: Indicates if the vulnerability has been fixed in the upstream component.
- **Installed Version**: Version currently included in the submitted APK.
- **Fixed Version**: Version where the vulnerability has been resolved.

> **Recommendation:** To eliminate known HIGH and CRITICAL vulnerabilities, upgrade each listed component to the version specified in the *Fixed Version* column.

2. Dependency Graph

This graph visualizes relationships between components, helping trace how vulnerable libraries are included in the APK—especially when they are *transitive dependencies* (i.e., indirectly included through other components).

The graph includes:

- All components with known HIGH or CRITICAL CVEs.
- All components that directly or transitively depend on them.

> **Purpose:** This visualization assists in identifying which parent components need to be updated to remove vulnerable dependencies from the APK.

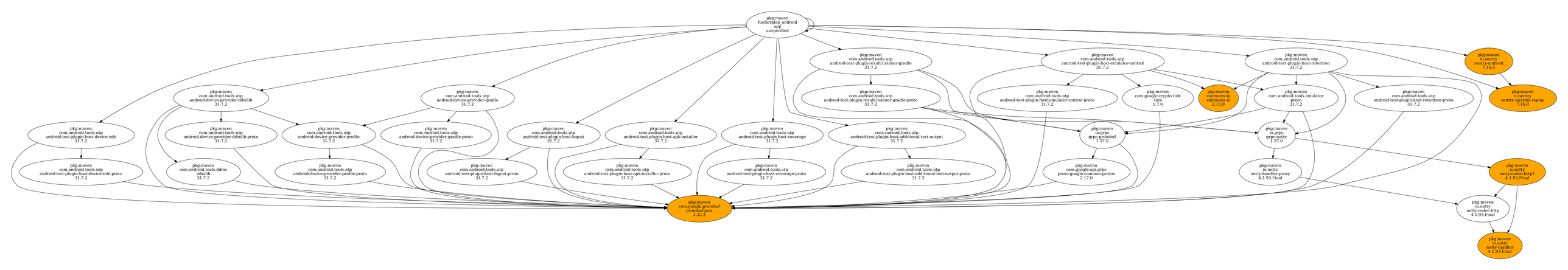
Report Summary

Target	Type	Vulnerabilities
Java	jar	7

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

Java (jar)
==========
Total: 7 (HIGH: 7, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
com.google.protobuf:protobuf-java	CVE-2024-7254	HIGH	fixed	3.22.3	3.25.5, 4.27.5, 4.28.2	protobuf: StackOverflow vulnerability in Protocol Buffers https://avd.aquasec.com/nvd/cve-2024-7254
commons-io:commons-io	CVE-2024-47554			2.13.0	2.14.0	apache-commons-io: Possible denial of service attack on untrusted input to XmlStreamReader https://avd.aquasec.com/nvd/cve-2024-47554
io.netty:netty-codec-http2	CVE-2025-55163			4.1.93.Final	4.2.4.Final, 4.1.124.Final	netty: netty-codec-http2: Netty MadeYouReset HTTP/2 DDoS Vulnerability https://avd.aquasec.com/nvd/cve-2025-55163
	GHSA-xpw8-rcwv-8f8p				4.1.100.Final	io.netty:netty-codec-http2 vulnerable to HTTP/2 Rapid Reset Attack https://github.com/advisories/GHSA-xpw8-rcwv-8f8p
io.netty:netty-handler	CVE-2025-24970				4.1.118.Final	io.netty:netty-handler: SslHandler doesn't correctly validate packets which can lead to native crash... https://avd.aquasec.com/nvd/cve-2025-24970
io.sentry:sentry-android	GHSA-7cjh-xx4r-qh3f			7.16.0	8.14.0	sentry-android unmasked sensitive data in Android Session Replays for users of Jetpack... https://github.com/advisories/GHSA-7cjh-xx4r-qh3f
io.sentry:sentry-android-replay						


pkg:maven
Rocketplan_android
app
unspecified
pkg:maven
com.android.tools.utp
android-test-plugin-result-listener-gradle
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-emulator-control
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-retention
31.7.2
pkg:maven
io.sentry
sentry-android
7.16.0
pkg:maven
com.android.tools.utp
android-device-provider-ddmlib
31.7.2
pkg:maven
com.android.tools.utp
android-device-provider-gradle
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-result-listener-gradle-proto
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-emulator-control-proto
31.7.2
pkg:maven
com.google.crypto.tink
tink
1.7.0
pkg:maven
commons-io
commons-io
2.13.0
pkg:maven
com.android.tools.emulator
proto
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-retention-proto
31.7.2
pkg:maven
io.sentry
sentry-android-replay
7.16.0
pkg:maven
com.android.tools.utp
android-test-plugin-host-device-info
31.7.2
pkg:maven
com.android.tools.utp
android-device-provider-ddmlib-proto
31.7.2
pkg:maven
com.android.tools.utp
android-device-provider-profile
31.7.2
pkg:maven
com.android.tools.utp
android-device-provider-gradle-proto
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-logcat
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-apk-installer
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-coverage
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-additional-test-output
31.7.2
pkg:maven
io.grpc
grpc-protobuf
1.57.0
pkg:maven
io.grpc
grpc-netty
1.57.0
pkg:maven
io.netty
netty-codec-http2
4.1.93.Final
pkg:maven
com.android.tools.utp
android-test-plugin-host-device-info-proto
31.7.2
pkg:maven
com.android.tools.ddms
ddmlib
31.7.2
pkg:maven
com.android.tools.utp
android-device-provider-profile-proto
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-logcat-proto
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-apk-installer-proto
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-coverage-proto
31.7.2
pkg:maven
com.android.tools.utp
android-test-plugin-host-additional-test-output-proto
31.7.2
pkg:maven
com.google.api.grpc
proto-google-common-protos
2.17.0
pkg:maven
io.netty
netty-handler-proxy
4.1.93.Final
pkg:maven
com.google.protobuf
protobuf-java
3.22.3
pkg:maven
io.netty
netty-codec-http
4.1.93.Final
pkg:maven
io.netty
netty-handler
4.1.93.Final