Security Report - Animals In Distress

Generated by Snyk Security Scanner

Project: Animals In Distress
Organization: st10382828
Scan Date: 2025-11-05 23:12:34
Snyk Project URL: https://app.snyk.io/org/st10382828/project/c4523e7d-e6d6-465f-b786-c46d2baaab86

Executive Summary

Metric	Count
Total Vulnerabilities	17
High Severity	10
Medium Severity	5
Low Severity	2
Total Dependencies Tested	319
Vulnerable Paths	145

High Severity Issues (10)

1. Stack-based Buffer Overflow in protobuf-javalite

- **Vulnerability**: SNYK-JAVA-COMGOOGLEPROTOBUF-9398723
- **Package**: `com.google.protobuf:protobuf-javalite@3.14.0`
- **Introduced by**: `com.google.firebase:firebase-firestore-ktx@25.1.1`
- **Fix Available**: Upgrade to versions 3.25.5, 4.27.5, or 4.28.2
- **Impact**: Stack-based buffer overflow can lead to arbitrary code execution

2. Stack-based Buffer Overflow in protobuf-java

- **Vulnerability**: SNYK-JAVA-COMGOOGLEPROTOBUF-8055227
- **Package**: `com.google.protobuf:protobuf-java@3.24.4`
- **Introduced by**: `com.google.testing.platform:android-driver-instrumentation@0.0.9-alpha03`
- **Fix Available**: Upgrade to versions 3.25.5, 4.27.5, or 4.28.2
- **Impact**: Stack-based buffer overflow vulnerability

3. Stack-based Buffer Overflow in protobuf-java-util

- **Vulnerability**: SNYK-JAVA-COMGOOGLEPROTOBUF-8055228
- **Package**: `com.google.protobuf:protobuf-java-util@3.22.3`
- **Introduced by**: `com.google.testing.platform:android-driver-instrumentation@0.0.9-alpha03`
- **Fix Available**: Upgrade to versions 3.25.5, 4.27.5, or 4.28.2
- **Impact**: Stack-based buffer overflow vulnerability

4. Denial of Service (DoS) in protobuf-javalite

- **Vulnerability**: SNYK-JAVA-COMGOOGLEPROTOBUF-3167771
- **Package**: `com.google.protobuf:protobuf-javalite@3.14.0`
- **Introduced by**: `com.google.firebase:firebase-firestore-ktx@25.1.1`
- **Fix Available**: Upgrade to versions 3.16.3, 3.19.6, 3.20.3, or 3.21.7
- **Impact**: DoS attack potential

5. Allocation of Resources Without Limits in netty-codec-http2

- **Vulnerability**: SNYK-JAVA-IONETTY-11799531
- **Package**: `io.netty:netty-codec-http2@4.1.93.Final`
- **Introduced by**: `com.android.tools.utp:android-test-plugin-result-listener-gradle@31.13.0`
- **Fix Available**: Upgrade to versions 4.1.124.Final or 4.2.4.Final
- **Impact**: Resource exhaustion attacks possible

6. Improper Handling of Highly Compressed Data in netty-codec-http2

- **Vulnerability**: SNYK-JAVA-IONETTY-12485151
- **Package**: `io.netty:netty-codec-http2@4.1.93.Final`
- **Introduced by**: `com.android.tools.utp:android-test-plugin-result-listener-gradle@31.13.0`
- **Fix Available**: Upgrade to version 4.1.125.Final
- **Impact**: Data amplification attacks possible

7. Denial of Service (DoS) in netty-codec-http2

- **Vulnerability**: SNYK-JAVA-IONETTY-5953332
- **Package**: `io.netty:netty-codec-http2@4.1.93.Final`
- **Introduced by**: `com.google.testing.platform:core@0.0.9-alpha03`
- **Fix Available**: Upgrade to version 4.1.100.Final
- **Impact**: DoS attack potential

8. HTTP Request Smuggling in netty-codec-http

- **Vulnerability**: SNYK-JAVA-IONETTY-12485149
- **Package**: `io.netty:netty-codec-http@4.1.93.Final`
- **Introduced by**: `com.android.tools.utp:android-test-plugin-result-listener-gradle@31.13.0`
- **Fix Available**: Upgrade to versions 4.1.125.Final or 4.2.5.Final
- **Impact**: HTTP request smuggling attacks possible

9. Improper Handling of Highly Compressed Data in netty-codec-http

- **Vulnerability**: SNYK-JAVA-IONETTY-12485150
- **Package**: `io.netty:netty-codec-http@4.1.93.Final`
- **Introduced by**: `com.android.tools.utp:android-test-plugin-result-listener-gradle@31.13.0`
- **Fix Available**: Upgrade to version 4.1.125.Final
- **Impact**: Data amplification attacks possible

10. Improper Validation of Specified Quantity in netty-handler

- **Vulnerability**: SNYK-JAVA-IONETTY-8707739
- **Package**: `io.netty:netty-handler@4.1.110.Final`
- **Introduced by**: `com.google.testing.platform:core@0.0.9-alpha03`
- **Fix Available**: Upgrade to versions 4.1.118.Final or 4.2.0.RC3
- **Impact**: Input validation issues

Medium Severity Issues (5)

1. Denial of Service (DoS) in protobuf-javalite

- **Vulnerability**: SNYK-JAVA-COMGOOGLEPROTOBUF-3040281
- **Package**: `com.google.protobuf:protobuf-javalite@3.14.0`
- **Introduced by**: `com.google.firebase:firebase-firestore-ktx@25.1.1`
- **Fix Available**: Upgrade to versions 3.16.3, 3.19.6, 3.20.3, or 3.21.7
- **Impact**: DoS attack potential

2. Allocation of Resources Without Limits in netty-codec-http

- **Vulnerability**: SNYK-JAVA-IONETTY-6483812
- **Package**: `io.netty:netty-codec-http@4.1.93.Final`
- **Introduced by**: `com.google.testing.platform:core@0.0.9-alpha03`
- **Fix Available**: Upgrade to version 4.1.108.Final
- **Impact**: Resource exhaustion attacks possible

3. Denial of Service (DoS) in netty-handler

- **Vulnerability**: SNYK-JAVA-IONETTY-5725787
- **Package**: `io.netty:netty-handler@4.1.93.Final`
- **Introduced by**: `com.google.testing.platform:core@0.0.9-alpha03`
- **Fix Available**: Upgrade to version 4.1.94.Final
- **Impact**: DoS attack potential

4. Denial of Service (DoS) in netty-common

- **Vulnerability**: SNYK-JAVA-IONETTY-8367012
- **Package**: `io.netty:netty-common@4.1.93.Final`
- **Introduced by**: `com.android.tools.utp:android-test-plugin-result-listener-gradle@31.13.0`
- **Fix Available**: Upgrade to version 4.1.115.Final
- **Impact**: DoS attack potential

5. Improper Validation of Specified Quantity in netty-common

- **Vulnerability**: SNYK-JAVA-IONETTY-8707740
- **Package**: `io.netty:netty-common@4.1.93.Final`
- **Introduced by**: `com.android.tools.utp:android-test-plugin-result-listener-gradle@31.13.0`
- **Fix Available**: Upgrade to versions 4.1.118 or 4.2.0.RC3
- **Impact**: Input validation issues

Low Severity Issues (2)

1. Information Exposure in kotlin-stdlib

- **Vulnerability**: SNYK-JAVA-ORGJETBRAINSKOTLIN-2393744
- **Package**: `org.jetbrains.kotlin:kotlin-stdlib@2.0.21`
- **Introduced by**: Multiple Kotlin dependencies
- **Fix Available**: Upgrade to version 2.1.0
- **Impact**: Information exposure risk
- **Affected Packages**:
  - `org.jetbrains.kotlin:kotlin-build-tools-impl@2.0.21`
  - `org.jetbrains.kotlin:kotlin-compiler-embeddable@2.0.21`
  - `org.jetbrains.kotlin:kotlin-klib-commonizer-embeddable@2.0.21`
  - `org.jetbrains.kotlin:kotlin-stdlib@2.0.21`

2. Creation of Temporary File in Directory with Insecure Permissions in guava

- **Vulnerability**: SNYK-JAVA-COMGOOGLEGUAVA-5710356
- **Package**: `com.google.guava:guava@31.1-android`
- **Introduced by**: `com.google.firebase:firebase-analytics-ktx@22.1.2`
- **Fix Available**: Upgrade to versions 32.0.0-android or 32.0.0-jre
- **Impact**: Temporary file security issues

Detailed Vulnerability Breakdown

By Dependency Type

Firebase Dependencies

- **Firebase Firestore**: 4 vulnerabilities (3 High, 1 Medium)
- **Firebase Analytics**: 1 vulnerability (Low)
- **Impact**: Core Firebase functionality affected

Kotlin Dependencies

- **Kotlin Standard Library**: 4 vulnerabilities (Low)
- **Impact**: Development/build tools affected

Testing Dependencies

- **Android Testing Platform**: 9 vulnerabilities (7 High, 2 Medium)
- **Impact**: Testing infrastructure only (not production)

Network Dependencies

- **Netty**: 8 vulnerabilities (6 High, 2 Medium)
- **Impact**: Network communication layer

Recommendations

Immediate Actions (High Priority)

1. **Upgrade Firebase Dependencies**
    - Update `firebase-firestore-ktx` to latest version
    - Update `firebase-analytics-ktx` to latest version
    - This will resolve 5 high/medium severity issues
2. **Upgrade Kotlin Dependencies**
    - Update Kotlin to version 2.1.0 or later
    - This will resolve 4 low severity issues

Medium Priority

3. **Update Testing Dependencies**
    - Most vulnerabilities are in testing-only dependencies
    - Update Android testing platform dependencies
    - Note: These don't affect production builds

Long-term Actions

4. **Regular Security Monitoring**
    - Use Snyk to monitor for new vulnerabilities
    - Set up automated alerts
    - Review security reports monthly
5. **Dependency Management**
    - Consider using dependency resolution strategies
    - Implement Gradle dependency locking
    - Regular dependency updates

Risk Assessment

Production Impact

- **High Risk**: 7 vulnerabilities in production dependencies (protobuf, netty)
- **Medium Risk**: 4 vulnerabilities requiring attention
- **Low Risk**: 6 vulnerabilities in development/testing tools

Application Context

- **Firebase Dependencies**: Used for core app functionality (Firestore, Analytics)
- **Netty**: Used by testing and build tools, not directly in production code
- **Kotlin**: Development dependency, affects build process

Mitigation Status

- All vulnerabilities are in transitive dependencies (dependencies of dependencies)
- Most can be resolved by updating parent dependencies
- Testing dependencies don't affect production builds

Additional Information

Scan Configuration

- **Package Manager**: Gradle
- **Target File**: `build.gradle.kts`
- **Projects Scanned**: 2 (root project + app module)
- **Open Source**: No

Continuous Monitoring

- **Snyk Project**: https://app.snyk.io/org/st10382828/project/c4523e7d-e6d6-465f-b786-c46d2baaab86
- **Monitoring Enabled**: Yes
- **Email Notifications**: Enabled for new vulnerabilities

Contact & Support

For questions about this security report:

- **Snyk Dashboard**: https://app.snyk.io/org/st10382828/project/c4523e7d-e6d6-465f-b786-c46d2baaab86
- **Snyk Documentation**: https://docs.snyk.io/
- **Organization**: st10382828

Report Generated: 2025-11-05 23:12:34
Scanner Version: Snyk CLI (latest)
Report Format: Markdown

This report was generated automatically by Snyk security scanner. For the most up-to-date information, please visit the Snyk dashboard.