Fortifying the Security Assurance Process Using Software Composition Analysis

Jason Gay  
Cybersecurity Engineer
Agenda

Introduction to Magna Electronics
Vehicle Systems and Open Source
Software Composition Analysis
Evaluation & Final Metrics
Summary
Magna Electronics Overview

AUTOMATED DRIVING SYSTEMS

SECURE CONNECTIVITY

ELECTRIFICATION
Agenda

Introduction to Magna Electronics

Vehicle Systems and Open Source

Software Composition Analysis

Evaluation & Final Metrics

Summary
Advanced Vehicle Systems

- Vehicles becoming more connected and automated
- Cybersecurity impacts become more critical
- Cybersecurity practices need to keep up
Magna Electronics Systems

- LED Lighting Systems
- Domain Controllers
- DCT and Hybrid Transmissions
- Front Camera
- Auxiliary Systems (Pumps, eFans, etc.)
- Front Lighting
- Actuators
- Secure Connectivity
- Power Closure Systems
- Rear Camera
- Rear Lighting
- Latches
- Hybrid and Electric Systems
- Inside / Outside Mirrors
- 4WD / AWD Systems
- RADAR & LiDAR
Open Source Software

- Open-Source software is widely utilized for connected applications
  - Speed up application development process
  - May increase exposure to certain types of risk
Agenda

Introduction to Magna Electronics

Vehicle Systems and Open Source

Software Composition Analysis

Evaluation & Final Metrics

Summary
What is Software Composition Analysis?

- **Software Composition Analysis tools:**
  - Generate a software Bill of Materials
  - Map open source components to vulnerabilities published in NVD
    - Identify and treat vulnerabilities earlier
    - Avoid costly design changes later
National Vulnerability Database

- Vulnerabilities reported as a CVE entry in the NVD
  - CVE: Common Vulnerabilities and Exposures
  - Government repository of vulnerability information
    - Managed by National Institute of Standards and Technology
    - Common Vulnerability Scoring System (CVSS)
Common Vulnerability Scoring System

Common Vulnerability Scoring System Version 3.0 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.0).

Base Score

**Attack Vector (AV)**
- Network (N)
- Adjacent (A)
- Local (L)
- Physical (P)

**Attack Complexity (AC)**
- Low (L)
- High (H)

**Privileges Required (PR)**
- None (N)
- Low (L)
- High (H)

**User Interaction (UI)**
- None (N)
- Required (R)

**Scope (S)**
- Unchanged (U)
- Changed (C)

**Confidentiality (C)**
- None (N)
- Low (L)
- High (H)

**Integrity (I)**
- None (N)
- Low (L)
- High (H)

**Availability (A)**
- None (N)
- Low (L)
- High (H)

Vector String - CVSS:3.1/AV:N/AC:L/PR:N/UI:L/R0/W/C:NL/I:NL/A:N

**Rating** | **CVSS Score**
---|---
None | 0.0
Low | 0.1 - 3.9
Medium | 4.0 - 6.9
High | 7.0 - 8.9
Critical | 9.0 - 10.0
Software Composition Analysis

- **Software Composition Analysis becomes increasingly valuable**
  - Can be used as an on-demand scan tool
  - Can be integrated into an automation server to periodically scan and report
  - Provides notifications when new relevant vulnerabilities are published
Agenda

Introduction to Magna Electronics

Vehicle Systems and Open Source

Software Composition Analysis

Evaluation

Summary
Overview

• Three SCA tools were evaluated based on a sample software project
  – Manual post-processing of the results

• Issues encountered
  – False identification of components
  – Misidentifying component version numbers
  – Incomplete coverage

• Developed scoring system to rate each tool’s effectiveness
  – Based on estimation of the value each report provides
Metrics Considered

Preliminary Metrics

- **Quantity of Accurate Matches**
  - Number of CVEs reported that were determined to be correctly identified our project

- **Composite accurate CVSS Scores**
  - Sum of every accurate CVE’s CVSS score

- **Quality of Reported Data**
  - Results sorted into Accurate Matches, False Matches, and Version Mismatches
Quantity of Accurate Matches

### Accurate Matches by CVSS Score

<table>
<thead>
<tr>
<th></th>
<th>Tool X</th>
<th>Tool Y</th>
<th>Tool Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>79</td>
<td>6</td>
<td>27</td>
</tr>
<tr>
<td>Med</td>
<td>127</td>
<td>39</td>
<td>41</td>
</tr>
<tr>
<td>Low</td>
<td>37</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>
Composite CVSS Scores

<table>
<thead>
<tr>
<th>Tool</th>
<th>Total CVSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool X</td>
<td>1,406.0</td>
</tr>
<tr>
<td>Tool Y</td>
<td>256.5</td>
</tr>
<tr>
<td>Tool Z</td>
<td>428.6</td>
</tr>
</tbody>
</table>
# Quality of Reported Data

## TOOL X
- **Accurate**: 16%
- **FALSE**: 3%
- **Version Mismatch**: 81%

## TOOL Y
- **Accurate**: 14%
- **FALSE**: 0%
- **Version Mismatch**: 86%

## TOOL Z
- **Accurate**: 0.5%
- **FALSE**: 0%
- **Version Mismatch**: 99%

### Table of Data

<table>
<thead>
<tr>
<th>Tool</th>
<th>Accurate</th>
<th>False</th>
<th>Version Mismatch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool X</td>
<td>243</td>
<td>50</td>
<td>1,236</td>
</tr>
<tr>
<td>Tool Y</td>
<td>50</td>
<td>0</td>
<td>305</td>
</tr>
<tr>
<td>Tool Z</td>
<td>78</td>
<td>1</td>
<td>14,790</td>
</tr>
</tbody>
</table>
Final Metrics
Final Metrics

• Two Final Metrics
  – Total Coverage (%)
    • Number of accurate matches (out of composite unique matches found by all 3 tools)
  – Weighted Quality
    • Single score using the following scoring system:

<table>
<thead>
<tr>
<th>Item</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate Vulnerability</td>
<td>+ [CVSS Score]</td>
</tr>
<tr>
<td>False Positives</td>
<td>-1 point</td>
</tr>
<tr>
<td>Version Mismatches</td>
<td>-0.1 point</td>
</tr>
</tbody>
</table>
Total Coverage

### Coverage of the 289 Unique CVEs

<table>
<thead>
<tr>
<th></th>
<th>Count</th>
<th>Coverage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool X</td>
<td>243</td>
<td>84.08</td>
</tr>
<tr>
<td>Tool Y</td>
<td>50</td>
<td>17.30</td>
</tr>
<tr>
<td>Tool Z</td>
<td>78</td>
<td>26.99</td>
</tr>
</tbody>
</table>

- **Tool X**: 243 (84.08%)
- **Tool Y**: 50 (17.30%)
- **Tool Z**: 78 (26.99%)
Weighted Quality

- Composite CVSS score represents positive value
- False positives and mismatched versions provide negative value

<table>
<thead>
<tr>
<th>Tool</th>
<th>Composite CVSS</th>
<th>False Positives</th>
<th>Version Mismatches</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool X</td>
<td>1,406.0</td>
<td>50</td>
<td>1,236</td>
<td>1,232.4</td>
</tr>
<tr>
<td>Tool Y</td>
<td>256.6</td>
<td>0</td>
<td>305</td>
<td>226</td>
</tr>
<tr>
<td>Tool Z</td>
<td>428.6</td>
<td>1</td>
<td>14,970</td>
<td>-1,069.4</td>
</tr>
</tbody>
</table>

Score = Composite CVSS - False Positives - (Mismatches/10)
Conclusion

- Decision was made clear after processing and organizing the results
- Rating template applied to other internal project scans

<table>
<thead>
<tr>
<th>Tool</th>
<th>Weighted Quality</th>
<th>Total Coverage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool X</td>
<td>1,232.4</td>
<td>84.08</td>
</tr>
<tr>
<td>Tool Y</td>
<td>226.0</td>
<td>17.30</td>
</tr>
<tr>
<td>Tool Z</td>
<td>-1,069.4</td>
<td>26.99</td>
</tr>
</tbody>
</table>
Introduction to Magna Electronics

Vehicle Systems and Open Source

Software Composition Analysis

Evaluation & Final Metrics

Summary
Summary

- Software Composition Analysis is a powerful piece of the Secure Development Lifecycle

- Results vary widely from tool to tool

- Having a clear approach will have a significant impact on evaluation time and resulting value
Thank you