ONAP SECCOM retrospectives

Pawel Pawlak, Amy Zwarico
Porto, June 14th
Anti-Trust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrustpolicy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.
Agenda

• Log4j fix implementation in Istanbul Maintenance Release
• Jakarta security status update
Log4j related vulnerabilities revealed in December’21 emphasized the challenges in open source supply chain management.

Upon Security Subcommittee request, ONAP community agreed to reprioritize efforts and develop a dedicated Istanbul Maintenance release that upgraded vulnerable Log4j versions to latest greatest 2.17.1.

Based on commercial NEXUS IQ tool used in ONAP for Software Composition Analysis (SCA) with weekly Jenkins jobs scans results reports, jira tickets were created for four ONAP projects that were affected with Log4j direct dependencies.

So how did it go? The individual projects were efficient at upgrading to log4j 2.17.1 and one project was able to remove a vulnerable repository from the release because its functionality was no longer needed.

Unfortunately, there were delays. It took some time for ONAP Operations Manager project to merge the code.

Furthermore, while waiting for the merge, we observed a major failure in CI/CD automation pipeline causing problem with SCA reports generation. It took 19 days plus escalations for LFN IT to solve the problem. In the end we were able to use the final scan output to show that none of the ONAP projects had log4j direct dependencies.
The project teams discovered false positives in the Nexus IQ output, labeling some transitive dependencies as direct. These were manually whitelisted, and a ticket was opened with Sonatype, the Nexus IQ vendor, to address the false positives.

The dependency inherited from OpenDayLight (ODL), an LFN project used in two ONAP projects, had to be resolved by ONAP developers because the ODL version with the log4j fix was delivered too late for the ONAP release.

The final step was for each project to document the fixes and transitive dependencies in the Release Notes. Creating documentation jira tickets for each project was helpful in tracking progress. The Istanbul Maintenance release was publicly available end of March’22...

Could we make it faster?

**with SBOM in place** we would know easily which projects are using directly log4j, faster merge and faster resolution of failing SCA scan jobs would definitely speed up the final check, and more focus on documentation would make us release faster as well. Last but not least, having an automated repo upgrade process in place would solve the issue "on the fly"... We learn, we adjust, we improve.
Jakarta security status update – GR 1/4

- **REQ-1067** COMPLETION OF PYTHON LANGUAGE UPDATE (v2.7 → v3.8) [link to scan](#)

<table>
<thead>
<tr>
<th>No</th>
<th>Project’s jira</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VFC-1915</td>
<td>Closed</td>
<td>Merge done</td>
</tr>
<tr>
<td>2</td>
<td>VFC-1914</td>
<td>Closed</td>
<td>Filebeat related</td>
</tr>
<tr>
<td>3</td>
<td>DCAEGEN2-3020</td>
<td>Closed</td>
<td>Cloudify components migrated to Python 3.6</td>
</tr>
<tr>
<td>4</td>
<td>OOM-2900</td>
<td>Open</td>
<td>Cassandra</td>
</tr>
<tr>
<td>5</td>
<td>INT-2034</td>
<td>Open</td>
<td>Robot</td>
</tr>
</tbody>
</table>
Jakarta security status update – GR 2/4

- **REQ-1068** COMPLETION OF JAVA LANGUAGE UPDATE (v8 → v11) – [link to scan](#)

<table>
<thead>
<tr>
<th>No</th>
<th>Project’s jira</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AAI-3413</td>
<td>closed</td>
<td>Exceptions: java 8 due to the janusgraph dependency</td>
</tr>
<tr>
<td>2</td>
<td>DCAEGEN2-3019</td>
<td>closed</td>
<td>Exceptions: upstream NIFI base images are still built on java8</td>
</tr>
<tr>
<td>3</td>
<td>SDNC-1651</td>
<td>closed</td>
<td>Fixed in Istanbul</td>
</tr>
</tbody>
</table>

- Cassandra – upstream container
- Umaintained: message-router, msb-discovery, msb-eag, msb-iag
- srimzi-zk-entrance – OOM related
Jakarta security status update – GR 3/4

- **REQ-1066** CONTINUATION OF PACKAGES UPGRADES IN DIRECT DEPENDENCIES
  - 299 recommended package upgrades
  - 73% of upgrades completed or requested waiver
    - 179 completed (60%)
    - 38 waivers requested and recommended (13%)
  - 82 updates not addressed
    - 4 projects did zero updates
    - 1 large project completed about half the updates
Jakarta security status update – GR 4/4

**REQ-1069 CONTINUATION OF CII BADGING SCORE IMPROVEMENTS FOR SILVER LEVEL**

- Improvements in Passing, Silver and progress to Gold
- Top five projects (50-83% towards Gold Badge): DCAE Runtime, Policy, DCAE, VVP and CPS

**Release Statistics**

<table>
<thead>
<tr>
<th>Level</th>
<th>R1 Amsterdam 2</th>
<th>R2 Beijing 31</th>
<th>R3 Casablanca 30</th>
<th>R4 Dublin 30</th>
<th>R5 El Alto 30</th>
<th>R6 Frankfurt 39</th>
<th>R7 Guillin 39</th>
<th>R8 Honolulu 42</th>
<th>R9 Istanbul 42</th>
<th>current 42</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>0 0 0 0 0 0 1 1 0 0</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
</tr>
<tr>
<td>80-100%</td>
<td>0 0 0 0 0 0 1 1 0 0</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
</tr>
<tr>
<td>60-80%</td>
<td>0 0 0 0 0 0 1 1 0 0</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
</tr>
<tr>
<td>40-60%</td>
<td>0 0 0 0 0 0 1 1 0 0</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
</tr>
<tr>
<td>20-40%</td>
<td>0 0 0 0 0 0 1 1 0 0</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
</tr>
<tr>
<td>0-20%</td>
<td>0 0 0 0 0 0 1 1 0 0</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
<td>0 0 0 0 0 0 1 1 0 0 1</td>
</tr>
</tbody>
</table>

- Improvements in Passing, Silver and progress to Gold
- Top five projects (50-83% towards Gold Badge): DCAE Runtime, Policy, DCAE, VVP and CPS
Jakarta security status update – improvements

• RACI chart for unmaintained projects
  — proposed process related to technical debt

• Automating the process to mitigate security threats quicker
  — Removed a lot of manual work, saved a lot of time
LF Networking

LFN Developer & Testing Forum