A comprehensive view of Software Bill of Materials

Lars Bendix, Lund University
Andreas Göransson, QCM
sneSCM.org

Agenda

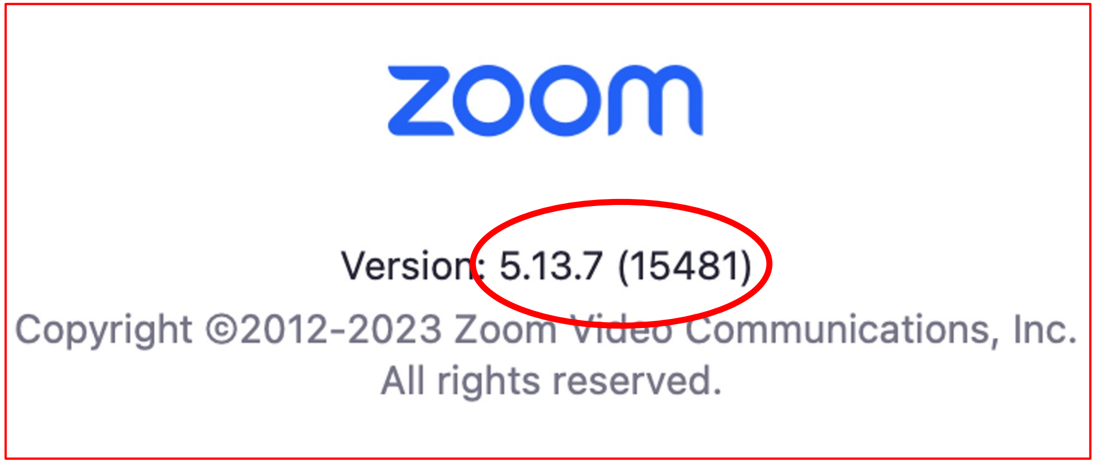
- DevOps SBoM motivation
- SBoM - Use Case categories
- General SBoM considerations
- Short Q&A

- RELEASE!

Motivation

- The US president made the general public interested in SBoM
- The NTIA stole SBoM away from us (SCM)
- (S)BoM has been used in SCM since the 1980’s
- SCM are the optimal producers of SBoMs
- External and **internal** users of SBoMs
- SBoM information is “fragmented”
- How you can use/exploit SBoM - the full story

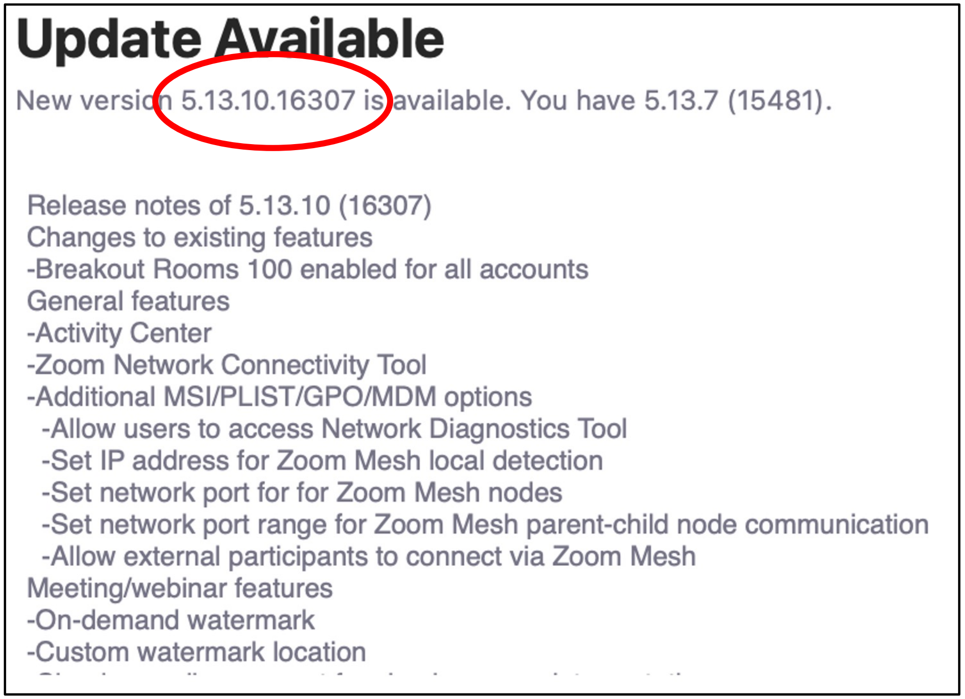
These are examples of SBoMs



zoom

Version: 5.13.7 (15481)

Copyright ©2012-2023 Zoom Video Communications, Inc.
All rights reserved.



Update Available

New version 5.13.10.16307 is available. You have 5.13.7 (15481).

Release notes of 5.13.10 (16307)
Changes to existing features
-Breakout Rooms 100 enabled for all accounts
General features
-Activity Center
-Zoom Network Connectivity Tool
-Additional MSI/PLIST/GPO/MDM options
 -Allow users to access Network Diagnostics Tool
 -Set IP address for Zoom Mesh local detection
 -Set network port for for Zoom Mesh nodes
 -Set network port range for Zoom Mesh parent-child node communication
 -Allow external participants to connect via Zoom Mesh
Meeting/webinar features
-On-demand watermark
-Custom watermark location

Overview - aspects and categories

- Materials aspect (BoM)
    - Search for object by UID
- Process aspect (BoP)
    - Use
    - **Troubleshooting**
    - Build
    - Build audit
- Information aspect (BoI)
    - Licence tracking
    - **Export control**
    - Legal aspects
    - Test-related matters
    - **Information sharing**

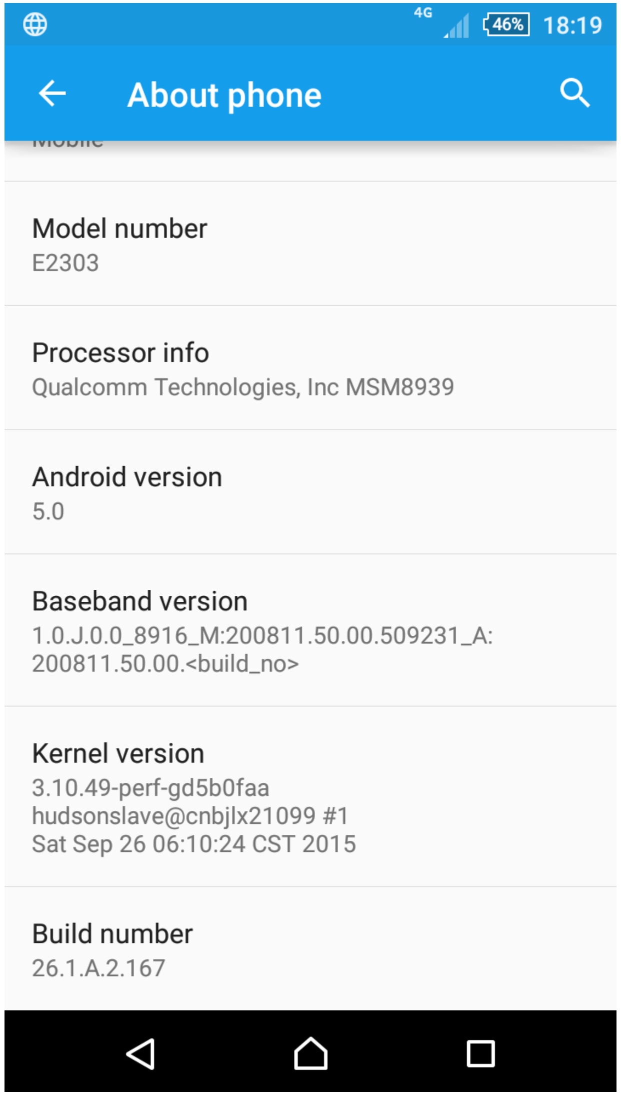
SBoM implementation considerations

- Level of detail of SBoM
- Availability of SBoM
- **Automation - both in creation and using**
- **Static and dynamic status of SBoM data**
- Keeping the SBoM up to date
- SBoM for tools and environments too - and Everything
- **SBoM and Microservices**
- Unique identifiers

Key takeaways

- SBoMs for **consumers**:
    - External consumers: List of ingredients & Vulnerability scan
    - Internal consumers: 100s of use cases, 10+ categories, 3 aspects
- SBoMs for **producers**:
    - “Builders” of a binary are at the origin of (most) SBoM data
    - Automation
    - Reproducibility
    - Static and dynamic status of data
- The “real” object and SBoM:
    - Configuration Item and data (attributes and relations)
    - Configuration Status Accounting

H&SBoM



About phone

Model number
E2303

Processor info
Qualcomm Technologies, Inc MSM8939

Android version
5.0

Baseband version
1.0.J.0.0_8916_M:200811.50.00.509231_A:
200811.50.00.<build_no>

Kernel version
3.10.49-perf-gd5b0faa
hudsonslave@cnbjlx21099 #1
Sat Sep 26 06:10:24 CST 2015

Build number
26.1.A.2.167

Q&A

https://fileadmin.cs.lth.se/cs/Personal/Lars_Bendix/Research/SBoM/