This is an update

• Draft now posted as a WG draft
• We are ready to go with editorial changes for -01 based on earlier feedback
• We still have some open questions.
Open Questions

• Is there a single SBOM or multiple SBOMs that are to be discovered?
• If there are multiple SBOMs, where do we apply an array?
• There is this other thing called “VEX” (Vulnerability Exploitability Exchange)
  • Common Vulnerability Reporting Format is one possible example.
  • http://docs.oasis-open.org/csaf/csaf-cvrf/v1.2/csaf-cvrf-v1.2.html
  • This answers the question: “Is this thing vulnerable to a particular CVE”?
  • There may be other formats in which this question is answered (CycloneDX)
  • Should we add this capability?
  • Key value: fewer phone calls when a device ISN’T vulnerable
More Open Questions

• We probably want to **remove** SWID references, add CycloneDX references, and maybe add one or two others as well

• Relationship to ROLLIE
Going forward

• How about doing something with this stuff at the IETF 111 Hackathon?
  • Interest?