VEX Working Group

SBOM-a-Rama

2024-02-29

Art Manion

zmanion@protonmail.com

https://groups.google.com/g/cisa-sbom-vex

Quick review: What is VEX?

Vulnerability Exploitability eXchange (VEX) indicates the status of a software product or component with respect to a vulnerability.

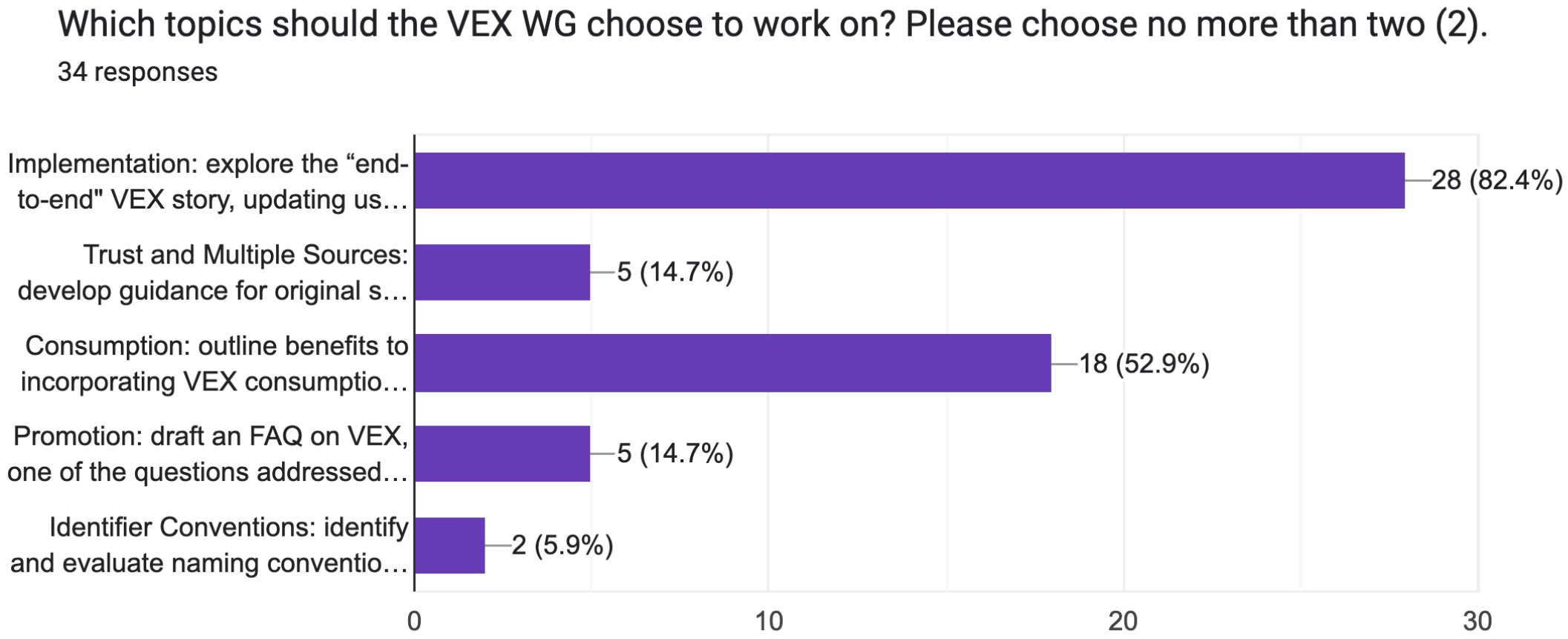
A common VEX use case is to indicate the status of a product or component with respect to a vulnerability.

- Not affected (with justifications), affected, fixed, under investigation
- Born from SBOM: How does a vulnerability in an upstream dependency affect this product?
- Works with SBOM, or independently
- Convey vulnerability status in a more standard way
- One vulnerability, one status, one or more components

VEX publications

- Vulnerability-Exploitability eXchange (VEX) – An Overview
  September 2021
- Vulnerability Exploitability eXchange (VEX) – Use Cases
  April 2022
- Vulnerability Exploitability eXchange (VEX) – Status Justifications
  June 2022
- Minimum Requirements for Vulnerability Exploitability eXchange (VEX)
  April 2023
- When to Issue VEX Information
  November 2023

What to work on next?



End-to-end VEX

Implementation: explore the “end-to-end" VEX story, updating use cases and documenting how things are done today

Consumption: outline benefits to incorporating VEX consumption into vulnerability management processes

How?

- Review current practices via semi-formal survey
- Analyze the results, what works, what doesn’t, user stories, process model, architecture

VEX practices review

What do we collectively really know about how VEX is being used?

- Ask actual VEX users!
- Survey template, Google form
- 18 responses, some presented and discussed at WG meetings
- Closing the survey period March 4 (probably)
- Point in time, do not plan to maintain current status of respondents

What did we learn?

Have not started the analysis phase yet, but some preliminary observations:

- Generally, VEX use is in early stage, more production than consumption, under evaluation and testing
- Fits well in automated vulnerability publication and management
- Some confusion about VEX status, particularly ”fixed” and “affected”
- Variety of formats in use
- SBOM integration desired but not common

Next steps

Analyze results

- Summarize responses, extract topics
- Develop user stories, VEX architecture?
- Identify significant issues, also what is working

Publish FTW!

VEX Working Group

SBOM-a-Rama

2024-02-29

Art Manion

zmanion@protonmail.com

https://groups.google.com/g/cisa-sbom-vex