Common Security Advisory Framework (CSAF) TC Working Session
Meeting Date: July 17, 2019
Time: 1:00 pm US EDT

1. Call to Order and Welcome

Meeting called to order @ 1:05 PM US EDT

2. Participants

2.1.1 Members Present

Company	Name	Role
Systems	Troy Fridley	Voting Member
Cisco Systems	Rhonda Levy	Voting Member
Cisco Systems	Omar Santos	Chair
Cisco Systems	Mike Gorski	Voting Member
Tibco Software	Eric Johnson	
AT&T	Patrick Maroney	Member
FireEye, Inc	Paul Patrick	Voting Member

5. Meeting Notes

- Omar—
  - Issues for 2.2.
    - **Omar** – regarding IDs in CVRF 1.2, support notes under bugs; the schema only supports one entry for ID - for anything, bug id or any reference.
      - Should we have more than one identifier?
      - Effects multiple platforms and follows multiple bugs. So, at minimal, would like opinions.
    - **Eric** – worth considering augmentation of original speck or a round trip of CVRF. Adding a field that has a list, means we can still do round trip, only one.
    - **Omar** –
      - but if someone creates a JSON version with multiples, we cannot convert to XML format.
      - Once in JSON format, adding additional properties such as: an array or Cisco bug ids, xml schema will reject and JSON will skip it.
      - Cisco bugs and an enumerated list would be compliant.
      - it will be under an ID. Another field.
    - **Eric** – we can label an id with a unique identifier. And can have multiple identifiers.
    - **Omar –** In this case, yes, we do.
    - **Eric** –

Some vulnerabilities have multiple IDs. The way CVRF is written for the content of CVRF.

- **Omar** its fine – good point – "Vendors can add specific bug identifiers outside of the 'id' field. The 'id' field will remain the same, as in CVRF 1.2. Or each bug ID can be a list of comma-separate."
- **Eric –**
    - part of spec for JSON schema could be to establish and identify x_Cisco. Trying to find value of that. Give vendors access? x_bug id? Or x_Cisco bug ids? Not sure that it matters.
    - There is optional content ID. Role up options. Grab role up id? Bug id tracking system in TIBCO – depends on other bugs.
    - Would create an umbrella ticket to include other bugs. Customers would just look at one bug.
- **Omar** – Godzilla and Red Hat – each bug ID had info on specific issues, version, etc.
- **Eric -** make sure all are fixed before going public.
- **Omar--**
    - Sometimes they are published before it is fixed.
    - The only thing we do is put bug IDs in notes. When we start documenting that vendor x ids. Don't have to change schema.
- **Eric** –
    - can be a list of identifiers. No constraint on that field. Comma separated list.
    - There is stuff that we can change. The task to get it done and we can get sidetracked. Opportunity to focus. Listen to tape.
- Eric's been working on a tool to convert XML CVRF documents into JSON.
    - Observations:
    - Some fields missing from JSON schema, and not in baseline schema. Some updates to JSON schema are forthcoming.
    - There are sample CVRS docs to exercise every aspect of schema. If empty, then no notes to list. Then must write out notes.
    - More value to TC to publish as open source or something where we contribute to Oasis as open projects or in GitHub.
- Omar –As long as some open source is included, then TIBCO can be used as an open repository; and can adopt standard perfectly fine.
    - Does TIBCO – has a preference?
    - Erick - No.
    - We want this to be in TIBCO'S repository. No preference.
- Eric – TIBCO has a strategy that we don't. We need a better open source strategy. In terms of what are looking at, writing in GO, a single repository is Git; and something that we would not like to add to. ??

  - Can make an Oasis an open project. Do not know if you have a preference. Probably TIBCO would want to make it under TIBCO software org.
- Omar –
  - From the previous experience we have had in the Cisco PSIRT repository, no objection internally.
  - Wanted to get straight and working before calling it a contribution. Probably – that stream may work.
  - Can have in TIBCO or your repository, and then forward for acceptance. If they say no, TIBCO, for there repository not a preference.
- Eric –
  - To complete the model in XML:
    - Write an independent model separate of XML,
      and change the structure of the document.
    - Add product tree and vulnerabilities, is the other step and includes stuff in XML group or product id – changed to a pointer.
    - Last challenge, JSON cannot validate XML, and has to be written in code.
    - Take JSON, parse JSON, map into platform, independent model, and get stuff to enforce.
    - Got the first XML setup complete. The platform is in independent format, then will write code to substantiate model and serialize that.
    - Then write in JSON format. Run test cases. A bunch of work to do, going through code line by line.
- Omar –
  - Did not expect so much work going involved in this project and appreciate that.
  - Has anyone looked at the schema and have feedback?
- Eric – will miss next meeting due to vacation.
- Eric –
  - It's an easy thing to post on GitHub.
  - A good place to start and then can host in Oasis.
  - It is an assumption that GitHub allows? Tricky.
  - Does know who to talk to and it is not that hard. Worked with Lawyers and they will get back to me. Doesn't concern me.
  - Probably not good to jump right to Oasis.

6. Next Meeting

Next Meeting will be a **monthly meeting** on Wednesday, August 14, 2019 at 1:00 PM US EDT