OASIS Common Security Advisory Framework (CSAF) TC Meeting #20 October 31, 2018

Chair: Omar Santos

Attendees:

- Anthony Bettini
- Art Manion
- Beth Pumo
- Chok Poh
- Denny Page
- Eric Johnson
- Feng Guest
- Jamison Day
- Jared Semrau
- Jonathan Bitle
- Langley Rock
- Lou Ronnau
- Lucas Tamagna-Dart
- Mike Gorski
- Rhonda Levy

1. Call to Order and Welcome

Meeting called to order @ 13:05 PM EST (17:05 UTC).

2. Roll call

All participants recorded their attendance on the OASIS meeting calendar - **quorum** was reached.

All participants were kindly encouraged to register themselves to optimize the use of the shared time during the meeting in one of two ways:

Either click the link with the text "Register my attendance" on the top of the event page or directly visit the per event direct "record my attendance link": https://www.oasis-open.org/apps/org/workgroup/csaf/record_my_attendance.php?event_id=46223&confirmed=1

2.1 Participants

2.1.1 Voting Members Present

Name	Company	Role
Bitle, Jonathan	Kaiser Permanente	Voting Member
Cao, Feng	Oracle	Voting Member
Day, Jamison	LookingGlass	Voting Member
Johnson, Eric	TIBCO Software Inc.	Voting Member
Page, Denny	TIBCO Software Inc.	Voting Member
Poh, Chok	Oracle	Voting Member
Pumo, Beth	Kaiser Permanente	Voting Member
Ronnau, Louis	Cisco Systems	Voting Member
Santos, Omar	Cisco Systems	Chair
Semrau, Jared	FireEye, Inc.	Voting Member

2.1.2 Members Present

- Mike Gorski, Cisco

2.1.3 Observers present

Note: Observers of this committee that are ready to become Members should follow the specific instructions displayed the OASIS Open Notices tab.

- None

2.2 Voting Right Changes Effective After the Meeting

2.2.1 Members who gained Voting Rights

- None

2.2.2 Members who lost Voting Rights

- None

3. Approval of Agenda

- After a review and brief discussion of the proposed agenda, Eric motioned for the agenda below to be approved. Seconded by Denny. Motion passes by unanimous agreement. Approved agenda with no modifications.

Agenda approved.

4. Approval of Minutes from Previous Meetings

- Meeting minutes for CSAF TC Monthly meeting #18 approved. Eric Johnson moved to approve the meeting minutes of meeting #18 Denny seconded. Unanimous consent, the motion carries, meeting minutes approved unchanged as published. Meeting #19 (September 2018) was cancelled.

5. MITRE'S CVE JSON CEBE Numbering Authority (CNA) update and adoption.

Art Mansion –data alignment maybe in CSAF, and would like to work on mapping names; however, no time to volunteer. They are all aware of each other CVE and CSAF.

Omar – agrees with points. Will share information by the end of next week. **Action item** to provide paring information. Products or product – will synch names.

Feng – First issue, Microsoft continues using CPE most vendors are not involved in product. Must update CVEs. Keep CVEs for a long time. Second issue, there are CVE pilot concerns from other participants; and for purposes of CSAF we create our own repository. There is a push or suggestion by MITRE's to sign commits. CSAF not included and most vendors have their own repositories.

Art – GitHub alternative servers are available. Feng agrees on value for CSAF. Discussion is intended for CSAF progress and commentary no decisions to be made at this time.

Enhancement of Generic Software Identification Parameter/Attribute to be included in CSAF 2.0 schema.

Omar: Currently we have support for CVE, within flexible or empty field references to a document or an XPDS. Don't have to have evolution of product. Will it take place of CVE or product? Or optional parameter?

Eric – would not CVRF – clearly a choice of CSAF, CVE – SWID id or CP reference or whatever it is; do we want it as part of JSON human references? Or stand alone? Mack OS 10.14.1 – exists do I put declaration in CSAF – Mojave? Meaningful by itself in CSAF – but a good reference to use outside? Loose definition? Let's be clear about how much redundancy are we embracing.

Feng – define types then they can put parameters there, and later they can change them.

Art – knee deep in NCIA – have not seen a speck change. Agrees with generic capability of field of reference of undetermined type. Human-readable fields should and cannot be disjointed with machine refence. However, it might be hard to inform.

Eric – generic field JSON a parent element, then formal description, and then other names can be used under it – optional values.

Denny – agree with what Art said about human readable being an important part of all of this. People are trying to evaluate advisories, wading through a SWID or summary, and going to another place to figure out what it is, is a very bad thing.

Art – "second guessing myself." JSON at core machine-readable format is used at Cisco and Oracle; it could be the case that an external generator can look them up.

Denny – great as optional – but to enforce SWID and others to line up, we should use caution about external references.

Omar – standards from vendors and external sources should have human-readable data. Second one, realistically not everyone will adopt the standard. Everyone agrees that conceptionally, within JSON format we should have human-readable language.

Eric – is there something that we can extract and have a compliance check for a JSON formatted document? If so, then fields must match a specific document.

Lucas – with CVE you would have to know who the vendor is, a Mac OS or whatever.

Eric – JSON should align and must align with CSAF. If they don't match, then it is an error. Can we go down that path?

Omar – yes, CP assignment that does not match is not a CSAF problem but very inconsistent. That verification would be very hard. All carry some name of a product. The SWID can be anyone and is typically a vendor but can be anyone with open source. All of them include an id identifier. If published somewhere it will assist with processing.

Eric – we want to drive better human alignment with SWID and CPE. With data behind those documents, we are hoping to just grab them. We can create definitions for SWIDs but not CPs.

Art – this would take some investigation. SWIDs may have a spot for human name, for example a list of products in CVRS – 10 products as vulnerable. Related to CVRF.

Omar – put on product template. Belongs with product.

Feng – They are different things product names and software id.

Art – in a product tree for CVRF a product unit is placed in the ID, not a separate field higher up. Product is where tags, strings, SWIDs, etc., are located. Version numbers are listed together.

Start the documentation of candidate Committee Specification Draft for CSAF 2.0.

Omar – The goal to have this done by calendar year. Another goal is to offer earlier next year. Can we do this in parallel?

Eric – JSON schema is one open area and JSON has not implemented the line change from the last meeting. Existing standard doesn't map well to JSON. Addressed 6 months ago and brought it up. Project specification should be documented last.

Art - not a JSON expert, but XML to JSON follows the XML philosophy. Don't want XML artifacts in JSON.

Eric – product tree mapping is not aligned. Will try and resurrect the work.

Art – thank you for doing the work.

Omar- prioritized addressed – 2.0 major change to JSON, items that we discussed before product identifications, CVSs 3.0 support. Hope there will not be a 3.1. should not have a big impact. 4.0 would have a big impact. Any other items to address? Better schema or idea of schema? No other items.

8. Next steps

- Omar looking at four products: CPE, SWID, XPDF, COSWIT four items that we have now. Omar to summarize the four on list and email to team. Or table and address later.

- Omar – call to action resurrection Eric will follow up with an email – not a JSON expert but can put us in touch with someone who is. We need more review of JSON files and the more eyes stronger. Call to action to peruse.
- Need more level of research – alignments with standards elements to include in CSAF.
- Could be more says Art. PURL might warrant investigation.

10. Next Meetings

10.1 Next Meeting

- Next Meeting #21 will be on Wednesday, November 28th - 01:00pm to 02:00pm ET (i.e. 2018-11-28 19:00 to 20:00 CET (UTC+1)).
- Self-Registration link (available from approx. 15 minutes before meeting start):

https://www.oasis-open.org/apps/org/workgroup/csaf/record_my_attendance.php?event_id=47737&confirmed=1

4.2 Other Subsequent Meetings

- All meetings monthly on last Wednesday during: `01:00pm to 02:00pm ET - 19:00 to 20:00 CET (UTC+1)`

11. Any other business

No other business

12. Adjourn

The meeting was adjourned at 14:00 PM EST (19:00 PM UTC).

Eric moved to adjourn, and Denny seconded the motion.