CWE/CAPEC Board Meeting #4

Tuesday February 9, 2021 @ 1000-1200 EDT

Members in Attendance

Alec Summers - MITRE (CWE/CAPEC, Board Moderator)
Alexander Hoole - Micro Focus
Andrew van der Stock
Bill Curtis – CISQ
Braione Pietro - Università degli Studi di Milano - Bicocca
Chris Eng - Veracode
Chris Levendis – MITRE (CVE)
Jason Fung - Intel
Jay Gazlay – DHS CISA
Jason Oberg - Tortuga Logic
Joe Jarzombek - - Synopsys
Marisa Harriston MITRE (CWE/CAPEC, Secretariat)
Paul Anderson - GrammaTech
Christopher Turner - NIST (NVD)

Review of Previous Action Items

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.02	Further discussion around the definition of terms, and on potential information fields to collect/maintain should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.08.06.04	Request clarification from MITRE's general counsel regarding the ability for a non-board member to request the contents of a private list through the Freedom of Information Act or the Patriot Act.	Drew Buttner	Completed	Assigned on 2020/08/06.
2020.08.06.08	Further discussion on the topics of press inquiries and press releases should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.08.06.09	Further discussion on the topics of a hardware-related Top 25, a data-protection view, and tagging CVEs with software vs hardware should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.09.14.01	Create and propose a potential charter for the CWE/CAPEC Board.	Andrew van der Stock Joe Jarzombek Paul Anderson	In Progress	Assigned on 2020/09/14.
2020.11.17.01	Create and propose a short policy to guide the use of Trello and the setting of an agenda.	Drew Buttner	Not Started	Assigned on 2020/11/17.

2020.11.17.02	Establish and maintain a topic release schedule for the next 4 releases, post on public website, do not include a hard date but rather a timeframe like Q1, include a note that minor releases in addition to this schedule are still possible.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.03	Create a proposal for a standardized content submission and tracking process enabling community visibility and shared effort into advancing submissions.	Kurt Seifried	Not Started	Assigned on 2020/11/17.
2020.11.17.04	Create a definition of scope that states what is allowed as part of CWE and what would be considered for rejection.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.05	Reach out to Irena Bojanova (NIST) for an update on Bugs Framework and schedule a talk with the CWE/CAPEC Board.	Drew Buttner	Not Started	Assigned on 2020/11/17.

Agenda with Discussion Summary

High Level Guidance for Complex Mapping

Responsibly party members shared that adding an origin field (e.g. hardware or software) to a CVE is reasonable based on conversations with various stakeholders. It was determined that CVE would be the best location for hosting. The idea has been pitched to the CVE board and the Quality Working Group for discussion of implementation details and process for possible inclusion in 5.0 schema.

Another member acknowledged that the new feature would need to be evangelized before full adoption takes place.

There was also conversation about the significance of the change in relation to waiting for the next major update for its release.

ACTION: A follow up email was sent to the Quality Working Group to revive conversation. The responsible party is also following up with Katie from the CVE board.

A) More on CVE to CWE Mapping Guidance

The moderator shared that the CWE team is developing documents for wider dissemination (touching on navigation, specifically for new users). A series of meetings have started taking place between organizations and the CVE Working Group to identify what is needed from the community. As a result, a one pager (process and best practices) and a larger document (from three different tactics related to a weakness) will be produced.

The group then had a conversation regarding the core requirements of a weakness and the most appropriate way of presenting the information. One member defined a weakness as a technical debt (something you have to address in the future). The moderator acknowledged the challenge of trying to keep pertinent details while increasing how consumability of the content.

One member suggested improving the search function. Another member shared the confusion between different filter options such as categories, technical debt, and weaknesses rather than being able to focus on relevant CWE and then seeing the actions that can be taken. A second member agreed on the broad nature of some categories, which are ultimately irrelevant. He also explained that another confusing piece for users is the idea that a node can have several parents in different views and recommended creating a one pager on how to set up views, categories etc. Finally, one member described the distinctions between the needs of a new user and more experienced users.

B) Filtered View Demo

The moderator took a few minutes to walk through how CWE's filters can work.

One member expressed that the Consequences filters seemed to be most useful and that the view felt like a very "top-down" approach but that overall, the setup was useful. Another member suggested enhancing the view so that users could type in tags dynamically.

ACTION: The moderator will share these documents with the group. Later, promoting the documents will become the focus. Start planning to enhance search function with a focus on filtering.

Standardized Content Submission

The moderator shared that the CWE team is developing a new webform ahead of next release. The form will be tied to a new GitHub repository.

Creation of a Potential Charter

The Responsible Party shared that the charter and bylaws are being split into two separate documents.

FOIA Requests from Non-Board Members

MITRE Counsel shared that Jay Gazlay is the only person who must comply with Freedom of Information Act (FOIA) requests from non-board members. MITRE can't provide a response on whether Jay's email is part of that requirement, but it would likely be up to DHS Counsel to make the determination.

Press Releases

The moderator briefed the board on recent press coverage and upcoming podcast opportunities on the program in general and the expansion into hardware. The members also had a conversation about how they can provide input on this content prior to publishing/launching. The moderator agreed and shared that with the addition of a new team member focused on strategic communication, there should be clearer conversations taking place when these opportunities arise.

A member asked how often requests from the press come in. The moderator replied that this typically happens a couple of times per year but that there has been an uptick around certain unique events such as the new methodology of the Top 20 or the hardware expansion. However, lead times can vary. The CVE representative said that it's ideal to have a CWE response versus a MITRE response.

One member suggested focusing on what is leading to some of the changes within the CWE Top 25 so that the community has more insights. Another member suggested explaining the Common Weakness Scoring System.

ACTION: MITRE will develop a process to notify the board of future opportunities in the event that members are interested in participating in the review process. A talking points document could be developed for guidance and consistency so that anyone could field requests. Andrew will share OWASP's social media policy which allows members of the community to post on their behalf, for the purposes of seeing another training example.

CWE Compatibility Program

- Discussion of potential agenda (Member suggestions)
    - Move 'what we would like to see for improvements' towards the end of the program
    - Need to address what are the challenges within the CWE effectiveness program
    - OWASP Top 10 shouldn't be used as benchmarks. This a very low-level standard, but there is a need for something that is easily achievable.
    - Topics ideas:
        - Broaden Top 25 session to more of a priorities conversation
        - Link to CVE from CWE; help describe why the community should care about CWE
        - Connection between CWSS and CVSS – is there room for improvement?
    - Who should be in attendance?
        - Vendors are important for assisting with education
        - However, having a panel with both vendors and users could be useful
        - Pivot from vendor focus to general "community" offering?
        - Initial meeting with vendors, then meet with users/community, and eventually reconvene with first group

        - Compatibility program should be informed by users; bring subset of biggest users for panel; Consider inviting specifically for Track 2 (Do customers really care about CWE?/CWE Clarity)
    - Market is moving towards using multiple tools for detecting flaws. How are CWEs being used across the broader landscape in conjunction with other tools?
    - Academic connection:
        - Setting up engagements to discuss taxonomies and setting up case studies for real world events

Open Discussion

Release Schedule

The moderator reminded the group of the current schedule (CWE-quarterly and CAPEC bi-annually).

A member was interested in formalizing the schedule (without providing exact dates) and communicating the topics of upcoming releases so that the board, vendors and users could feel more prepared and contribute as appropriate.

Another member requested receiving information on future releases 1 to 2 releases ahead of time for vendors and potentially more time for board members.

The moderator shared that new releases generally consist of one or more new views, a set of new weaknesses, sometimes tree restructuring of the taxonomy. However, this doesn't necessarily apply to the hardware expansion side. We don't currently have a clear sense of what CWE 5.0 will include.

ACTION: Provide CWE Board with more information on 5.0 release for input.

Item Number	Action Item	Responsible Party	Status	Comments
2020.08.06.02	Further discussion around the definition of terms, and on potential information fields to collect/maintain should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.08.06.08	Further discussion on the topics of press inquiries and press releases should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.08.06.09	Further discussion on the topics of a hardware-related Top 25, a data-protection view, and tagging CVEs with software vs hardware should be had via the board mailing list.	ALL	Not Started	Assigned on 2020/08/06.
2020.09.14.01	Create and propose a potential charter for the CWE/CAPEC Board.	Andrew van der Stock Joe Jarzombek Paul Anderson	In Progress	Assigned on 2020/09/14.
2020.11.17.01	Create and propose a short policy to guide the use of Trello and the setting of an agenda.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.02	Establish and maintain a topic release schedule for the next 4 releases, post on public website, do not include a hard date but rather a timeframe like Q1, include a note that minor releases in addition to this schedule are still possible.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.03	Create a proposal for a standardized content submission and tracking process enabling community visibility and shared effort into advancing submissions.	Kurt Seifried	Not Started	Assigned on 2020/11/17.
2020.11.17.04	Create a definition of scope that states what is allowed as part of CWE and what would be considered for rejection.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.05	Reach out to Irena Bojanova (NIST) for an update on Bugs Framework and schedule a talk with the CWE/CAPEC Board.	Drew Buttner	Not Started	Assigned on 2020/11/17.
2020.11.17.06	Work on proposal that can be brought to both the CVE and CWE/CAPEC Boards about high-level guidance for complex mapping between vulnerabilities and HW+SW weaknesses as well as the chaining relationships that may exist.	Jason Fung Jason Oberg Chris Turner	In Progress	Assigned on 2020/11/17.

2021.02.10.01	Have CWE Board review Guidance documents and develop promotion plan.	Alec Summers	Not Started	Assigned on 2021/02/10.
2021.02.10.02	Develop a process to notify the board of future opportunities in the event that members are interested in participating in the review process. A talking points document could be developed for guidance and consistency so that anyone could field requests.	Alec Summers	Not Started	Assigned on 2021/02/10.