



## **CVE Board Meeting Notes May 11, 2022 (9:00 am – 11:00 am ET)**

### **CVE Board Attendance**

- ☐ Ken Armstrong, EWA-Canada, An Intertek Company
- ☒ Tod Beardsley, Rapid7
- ☒ Chris Coffin (MITRE At-Large), The MITRE Corporation
- ☐ Jessica Colvin
- ☒ Mark Cox, Red Hat, Inc.
- ☐ William Cox, Synopsys, Inc.
- ☐ Patrick Emsweller, Cisco Systems, Inc.
- ☐ Jay Gazlay, Cybersecurity and Infrastructure Security Agency (CISA)
- ☐ Tim Keanini, Cisco Systems, Inc.
- ☒ Kent Landfield, Trellix
- ☒ Scott Lawler, LP3
- ☒ Chris Levendis (MITRE, Board Moderator), CVE Program
- ☒ Art Manion, CERT/CC (Software Engineering Institute, Carnegie Mellon University)
- ☐ Pascal Meunier, CERIAS/Purdue University
- ☐ Tom Millar, Cybersecurity and Infrastructure Security Agency (CISA)
- ☐ Ken Munro, Pen Test Partners LLP
- ☒ Chandan Nandakumaraiah, Palo Alto Networks
- ☐ Kathleen Noble, Intel Corporation
- ☒ Lisa Olson, Microsoft
- ☒ Shannon Sabens, CrowdStrike
- ☒ Takayuki Uchiyama, Panasonic Corporation
- ☒ David Waltermire, National Institute of Standards and Technology (NIST)
- ☐ James “Ken” Williams, Broadcom Inc.

### **MITRE CVE Team Attendance**

- ☒ Kris Britton
- ☒ Christine Deal
- ☒ Dave Morse
- ☒ Art Rich



## Agenda

- 9:00-9:05 Introduction
- 9:05-10:35 Topics
  - Proposal to Run a GitHub Repository
  - Global Security Vulnerability Summit (GSVS) CVE Engagement
  - Open Discussion
- 10:35-10:55 Review of Action Items
- 10:55-11:00 Closing Remarks

## New Action Items from Today's Meeting

| Action Item # | New Action Item                                                                             | Responsible Party                 | Due |
|---------------|---------------------------------------------------------------------------------------------|-----------------------------------|-----|
| 05.11.01      | Send out a Doodle poll to identify a date for the first meeting of the repo rules document. | Secretariat                       |     |
| 05.11.02      | Develop initial outline of repo rules and distribute to the Board.                          | Art M.                            |     |
| 05.11.03      | Develop repo rules document and present to the Board for approval.                          | Chris L.<br>Kent L.<br>Shannon S. |     |

## Proposal to Run a GitHub Repository (Repo) (Art Manion)

- The proposal was to create a central repository (repo) for the CVE community to raise issues, questions, and discussion topics not already addressed in program documentation.
  - The initial proposal was for a GitHub repo, but a final determination is TBD.
  - Board consensus was they liked the idea, so it will move forward.
- The repo would be an open forum to promote transparency about how the program works, and allow searches on prior issues, questions, and topics.
- Whether GitHub or another option is used for the repo, the hosted site needs to have a connection to the CVE Program (i.e., not a personal site).
- The consensus of the Board was the repo needs committed resources.
  - Art M., Tod B., and Dave W. volunteered to operate/manage the repo.
  - There was concern about the risk of getting a higher volume of repo activity than current resources can handle.
- A desired feature of the repo is the ability to close out a thread when it is resolved, or continued discussion becomes non-productive.
- An initial step is to create repository rules to explain how to use the repo, the nature of acceptable topics, and rules of engagement in the repo forum.
  - **Action:** Art M. volunteered to create an initial outline of the rules document.



- Chris L., Kent L., and Shannon S. volunteered to start building the new rules document.
  - **Action:** The Secretariat will send out a Doodle poll to identify a date for the first meeting for the repo rules document.
  - **Action:** When complete, present the repo rules to the Board for approval.
- The Outreach and Communications Working Group (OCWG) will take the lead for operations and management of the repo, once launched.
  - This comes with the understanding that the program will work with OCWG to provide additional resources if needed.

### **Global Security Vulnerability Summit (GSVS) CVE Engagement (Art Manion)**

- The GSVS is scheduled for June 24, 2022, and Art M. will have a presentation to provide information about the CVE Program to generate interest to join the CVE community.
- Some program history will be presented, but the focus of the presentation will be on the CVE future, for example:
  - CVE Services rollout and JSON 5.0.
  - Program emphasis on reducing transaction burden on CNAs.
- Documentation about program history and current affairs will be sent to Art M.
  - A paper Chris L. wrote at the start of the Transition Working Group (TWG).
  - Lisa O. will send examples of cloud vulnerabilities where Microsoft has issued CVE IDs.

### **Open Discussion (out of time)**

#### **Review of Action Items**

- 09.03.04 (Dispute policy/process). Draft is complete, and a meeting with Secretariat to review the draft is scheduled for later today. After that, the next reviews will be QWG and SPWG, followed by presentation to the Board.
- 10.26.01 (Dispute tagging). The tag location on a CVE record and the tag format are known. Still need to define the tagging process. Coordinate and complete this action item with the completion of the Dispute policy/process (09.03.04).
- 10.28.01 (WG Operations Handbook). Chris L. and Christine D. will do a final review/edit. The next review will be by the WG chairs. The CNACWG chair will share the document with CNAs for their comments (must be a time-bound review).
- 12.16.01 (WG-to-WG comms). Tied to WG Ops Handbook (10.28.01). Both should be closed at the same time.
- 03.03.02 (CNA assignment for insecure default configurations). This is **closed**/removed from the action item list. It will be added to the list of future Board agenda topics. Secretariat will write up a summary of the issue and Chris L. will assign to a MITRE team member to work the details.
- 04.14.02 (CNA guidance to adopt new CVE Services). This is part of the overall CVE Services communications strategy and is on-going. TWG is also assisting with comms messages. Need to wait for operational CVE Services.



- 06.23.01 (2021 vision/historical paper). Chris L. and Christine D. will meet to add metrics and finalize.
- 06.23.01 (2021 state of the CVE Program annual report). Complete action item 06.23.01 (vision paper) first. Target publication of annual report is end of calendar year 2022. Finish what can between now and end of year, so can add late year information and publish quickly.
- 11.10.04 (Road show slides, part of CVE branding message). Chris L. will update the slides to include information about new CVE services.
- 02.02.03 (Enhance ‘lightening’ talk slides). This is **closed**/removed from the action item list. Combine with 11.10.04.
- 06.09.01 (Reach out to Terry McDonald for QWG participation re: STIX). Change status to on-hold, low priority.
- 01.19.02 (Reach out to STIX in OASIS). Related to action item 06.09.01. Change status to on-hold, low priority.
- 10.26.02 (CNA on-boarding experience). Check with Tod B. at next Board meeting about status.
- 11.10.05 (Share survey results of CNA on-boarding). This is **closed**/removed from the action item list. Combine with 10.26.02.
- 10.26.03 (Table top exercise for new vulnerabilities). This is intended for the summit. Align development with the summit schedule.
- 02.02.01 (Draft dispute policy). This is **closed**/removed from the action item list. Repetitive with action item 09.30.04.
- 02.02.02 (Google and GitHub re: fuzzing results). Change status to on-hold, pending CVE Services roll-out.

### Next CVE Board Meetings

- Wednesday, May 25, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, June 8, 2022, 9:00am – 11:00am (ET)
- Wednesday, June 22, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, July 6, 2022, 9:00am – 11:00am (ET)

### Discussion Topics for Future Meetings

- CVE Services updates, as needed
- Summit planning updates
- CVE Program website transition progress, as needed
- Council of Roots meeting highlights
- Working Group updates, every other meeting
- Researcher Working Group proposal for Board review
- Vision Paper and Annual Report
- Initiate Board vote for a proposed solution to allow CNAs to assign IDs for insecure default configuration (from closed action item 03.03.02).