CVE Board Meeting Notes

February 7, 2024 (9:00 am – 11:00 am EST)

Agenda

- Introduction
- Topics
    - kernel.org CNA Onboarding Discussion
    - Tally to Date of Nominations for CNA Board Liaison
    - Board Discussions and Voting Process (postponed)
    - Root Pipeline Status Update and Discussion
- Open Discussion
- Review of Action Items
- Closing Remarks

New Action Items from Today's Meeting

Action Item #	New Action Item	Responsible Party	Due
	Nothing to report	**Secretariat**	

kernel.org CNA Onboarding Discussion

- Federation necessitates onboarding CNAs with experience and those that can propose the best way to perform vulnerability determination. Kernel.org is a recently onboarded CNA that fits this need. They have demonstrable expertise in determining vulnerabilities related to the Linux kernel. Their approach is data-driven and automated.
- Any help or coordination identifying vulnerabilities is welcome.
- By law and policy, kernel.org must do all CVE work on personal time (volunteer basis).
- Value of kernel.org as a CNA:
    - Furthers the long-standing goal of adoption, incentivizes other organizations within the Linux Foundation to join the CVE Program (and likely will be a catalyst for open source organizations outside of the Linux Foundation to join the program)
    - Furthers our federated governance and operational strategy, and it moves security further left of boom.
- A member mentioned that the program has discussed in the past building a better channel for direct CNA-to-CNA communications, but nothing has happened to move that forward. We should reconsider that. The program has tried twice in the past seven years to put together a list of contacts for direct CNA to CNA communications. Some are willing to do that, and others are not. What does seem to work is CNAs identifying their own contacts. This may be something to bring up/introduce at VulnCon. Get ideas about how best to do this.
- A member mentioned that managing CNA scope is incredibly complicated.

Tally to Date of Nominations for CNA Board Liaison

- The voting period for the new Liaison closes COB Thursday, February 8 (EST). Once that is over, the votes will be tallied, results will be shared with the Board, and an announcement will be distributed on the list. There are two nominees.
- The number of responses received to date has been disappointing. In addition to the initial call for vote, there have been three reminder emails sent, and another will be sent today. Each email has included the bios for the two candidates.
- The idea was mentioned to consider using VulnCon as a forum for identifying nominees or maybe even voting. Another idea was to hold a town hall with the nominees. These will be considered for the future.
- There was discussion a few years ago about defining requirements for the nominees for Liaison, but it was concluded that CNAs should be able to elect their Liaison based on what they care about, and not necessarily a nominee's qualifications.
- Per the CNACWG Charter, CNAs may also select who they want for Chair. They may be the same person as the Liaison, but it does not have to be.

Root Pipeline Status Update and Discussion

- The Root Pipeline on Monday.com is used to coordinate onboarding of prospective CNAs. Each of the Top-Level Roots and Roots has access, managing their leads through onboarding to announcement as CNAs.
- In the case of the MITRE TL-Root, leads are entered into the Pipeline as soon a request is received. Other Roots may wait until they have had some communication with the prospect or receive their completed registration form before adding to the Pipeline.
- The Pipeline is a transparent coordination forum with Roots able to see each other's prospects and progress. If a prospect CNA is root shopping, the Pipeline enables early identification of the problem.
- Root shopping example: CNA lead identifies a Root, but the Root does not think their business model is good for the program. The lead, without telling anyone they were previously turned down, may then approach another Root to try to get into the program.
- As soon as the new CNA is announced, their entry is moved from the Pipeline over to the master board. The master list is the official copy of CNA's information, their contacts and scope and so on. The Secretariat manages this.
- Metrics can be generated from Pipeline data; e.g., leads that have gone through onboarding.
- It was agreed that the preferred approach is that when a completed registration form is received, the Board will be notified; the Secretariat will send an email to the private list. The Secretariat will work on automating this with Monday.com. It was noted that the email notice should have a predictable subject line.

Open Discussion

- Out of time.

Review of Action Items

- Out of time.

Next CVE Board Meetings

- Wednesday, February 21, 2024, 2:00pm – 4:00pm (EST)
- Wednesday, March 6, 2024, 9:00am – 11:00am (EST)
- Wednesday, March 20, 2024, 2:00pm – 4:00pm (EDT)

- Wednesday, April 3, 2024, 9:00am – 11:00am (EDT)
- Wednesday, April 17, 2024, 2:00pm – 4:00pm (EDT)
- Wednesday, May 1, 2024, 9:00am – 11:00am (EDT)

Discussion Topics for Future Meetings

- Board discussions and voting process
- Sneak peek/review of annual report template SPWG is working on
- Bulk download response from community about Reserved IDs
- CVE Services updates and website transition progress (as needed)
- Working Group updates (every other meeting)
- Council of Roots update (every other meeting)
- Researcher Working Group proposal for Board review
- Vision Paper and Annual Report
- Secretariat review of all CNA scope statements
- Proposed vote to allow CNAs to assign for insecure default configurations
- CVE Communications Strategy