



CVE Board Meeting, November 10, 2021

Members of CVE Board in Attendance

- Ken Armstrong, [EWA-Canada, An Intertek Company](#)
- Tod Beardsley, [Rapid7](#)
- Chris Coffin, [The MITRE Corporation](#) (MITRE At-Large)
- Jessica Colvin [JPMorgan Chase](#)
- Mark Cox, [Red Hat, Inc.](#)
- William Cox, [Synopsis, Inc.](#)
- Patrick Emsweller, [Cisco Systems, Inc.](#)
- Jay Gazlay, [Cybersecurity and Infrastructure Security Agency \(CISA\)](#)
- Tim Keanini, [Cisco Systems, Inc.](#)
- Kent Landfield, [McAfee Enterprise](#)
- Scott Lawler, [LP3](#)
- Chris Levendis, [CVE Program](#) (CVE Board Moderator)
- Art Manion, [CERT/CC \(Software Engineering Institute, Carnegie Mellon University\)](#)
- Pascal Meunier, [CERIAS/Purdue University](#)
- Ken Munro, [Pen Test Partners LLP](#)
- Tom Millar, [Cybersecurity and Infrastructure Security Agency \(CISA\)](#)
- 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.](#)

Members of MITRE CVE Team in Attendance

- Jo Bazar
- Kris Britton
- Christine Deal
- Jonathan Evans

Agenda

- | |
|---|
| 2:00-2:05: Introductions and Roll Call |
| 2:05-3:35: Open discussion items |
| 3:35-3:55: Review of Action items (see attached excel file) |
| 3:55-4:00: Wrap-up |

New Actions items from today’s Board Meeting



See attached Excel spreadsheet for open action items from prior meetings (CVE Board Meeting 10Nov21–Agenda and Action items.xls)

#	Action Item	Responsible Party	Due	Status	Comments
11.10.01	Research how the CVE Program can “chip away” at the 12-13% of CNAs who have never assigned CVE IDs and report back to the Board	Secretariat		Not Started	Assigned on 11/10/2021
11.02.02	Schedule onboarding session with VulDB	CNA Coordination Team		Not Started	Assigned on 11/10/2021
11.02.03	Cancel Board meetings for November 24 (Thanksgiving) and December 22 (Christmas)	Secretariat		Completed	Assigned on 11/10/2021
11.10.04	Send out “road show” set of slides to the Board for review and comment (to add CVE branding message)	Chris L.		Not Started	Assigned on 11/10/2021
11.10.05	Share survey feedback regarding onboarding with Roots	Secretariat		Not Started	Assigned on 11/10/2021

Discussion Items

- **Inactive CNAs: CNA1, CNA2, CNA3**
 - CNA Coordination team has done its due diligence regarding trying to establish communication and following the Inactive Policy.
 - CNA Coordination Team contacted someone from CNA1 via LinkedIn and he will let his colleagues know to contact the CVE Program. Recommend not revoking status as CNA yet, in the hopes that contact can be re-established
 - We started the notification process over with CNA2 on November 4 when we received new POCs. Recommend not revoking status as CNA yet, in the hopes that contact can be established with new POCs
 - Communication was established with CNA3, but they have failed to provide working links to their public advisory location and vulnerability disclosure policy. Recommend revoking their status as a CNA
 - No Board members opposed the recommendations of the CNA Coordination team indicated above
 - Board members discussed that the program should do more to ensure that CNAs are assigning CVEs (a skill not practiced is lost). Is there more the program can do to help CNAs understand the value of assignment? Seems to be a gap in our educational/training materials



- May be as simple as telling CNA prospects that there is no value to their participation in the program if they do not assign any CVE IDs
- According to MITRE, 25 CNAs have never having assigned a CVE ID (3 from 2018; 8 from 2020; 14 from 2021). In other words, 12-13% of CNAs have never assigned a CVE ID
- Board suggests that the CNA Coordination Team reach out to have a conversation with CNAs who have been around a while but have not assigned CVE IDs—do some root cause analysis
- ACTION: Secretariat will do some research and report back to the Board how we can reasonably chip away at the 12-13% of CNAs who have never assigned a CVE ID
- **CNAs to review their up-converted records before deployment**
 - TWG recommends that there be a five day review period for CNAs to review their upconverted data from (JSON 4 to 5). No Board members disagree with this timeframe.
 - Unless a systemic problem is revealed (during testing), deployment of the services should not be delayed (we can work out problems over time).
 - AWG would suggest posting a JSON 5.0 repository on GitHub for this review is the best, most expedient answer from a development perspective.
 - We have to tell people what to review, the purpose, the time limit (five days), provide a means for them to report the results, and if there are issues, a means by which the issue can be resolved and they can be made aware of the resolution.
 - During this review, CNAs will not have the ability to fix any of their data; they can fix it once it goes public.
 - This testing period would be to identify any systemic issues with the upconverter.
 - Suggestion was made that we have a soft launch for the services where we do not advertise that the services have been launched but we give the CNAs access to change things for a period of time. MITRE stated we are well positioned to do that if we want (because we have decided to support the GitHub submission pilot and JSON 4 until June); it's just a matter of marketing.
 - Board members on the call were polled to see, by a show of hands, if they agree to a two week soft launch period: 9 out of 11 Board members on the call raised their hand.
 - Details of the five day testing of upconverted data and the soft launch will be discussed at a WG Chair meeting following the Board meeting
- **QWG status on JSON 5 release candidate 5 (Accept pull request)**
 - JSON 5 rc 5 has been released and is ready for development
- **Recommendation for VulDB**
 - SPWG recommends allowing VulDB to become a CNA
 - No opposition on the Board call (9 out of 11 present raised their hand)
 - They will be onboarded as a CNA
 - ACTION: CNA Coordination Team schedule onboarding session
- **CVE Board Meeting Schedule for the rest of 2021**
 - Does the Board want to cancel or moving any of the meeting below?
 - Wednesday, November 24, 2021 9:00am-11:00am (EST)--**CANCEL**
 - Wednesday, December 8, 2021 2:00pm-4:00pm (EST)
 - Wednesday, December 22, 2021 9:00am-11:00am (EST)-**CANCEL**
 - Wednesday, January 5, 2022 2:00pm-4:00pm (EST)
 - ACTION: Secretariat to issue cancellations for November 24 and December 22 meetings
- **CVE Board Charter 3.4 - APPROVED!**
 - CVE Board Charter will be posted on the CVE Website November 16, 2021.
- **Cloud Vulnerabilities (See 3 steps below)**



- If there is interest in QWG, they will try to figure out how we will assign for cloud based vulnerabilities (define use cases in terms of value)
- **CVE Branding**
 - Explain the CVE ID story better to the general public
 - We are 25 years or so down the road and we still have not done a good job (if at all) of convincing people that CVE IDs are valuable
 - Program can do a blog, podcast, etc., to tell the story better. We will need volunteers for this story
 - Board members suggested we need more than just blogs—this message needs to be part of a marketing campaign. CNAs need something to argue/present to their management to show how the value of being part of the CVE Program
 - The message should be that CNAs participating in CVE and assigning CVE IDs display maturity by revealing vulnerabilities and assigning CVE IDs (it is a badge of honor because it shows your commitment to product security). This should be at the core of our brand.
 - In addition, any discussion or presentation can be put up against the current level of cyber attacks in the world; our message should be that companies who are transparent and identify their vulnerabilities are protecting the world. Do your part!
 - The suggestion was made to seek some volunteer marketing folks from our community
 - There are some preliminary steps the CVE Program needs to take: Chris L would like to share his “road show briefing” with the Board so that they can review, edit, and add the core branding message. Once this step is done, THEN we go to the marketing folks and the graphics people. We do not have to start from scratch.
 - ACTION: Chris will send out his briefing to the Board for review/comment.
- **Open Discussion: ADP Pilot**
 - At the next SPWG meeting, the ADP pilot will be add an agenda item (November 15) meeting to re-visit the ADP Pilot. MITRE would like to participate in the ADP pilot as an ADP in order to contribute references.

Next CVE Board Meetings

- Wednesday, November 24, 2021 9:00am-11:00am (EST) - CANCELED
- Wednesday, December 8, 2021 2:00pm-4:00pm (EST)
- Wednesday, December 22, 2021 9:00am-11:00am (EST) - CANCELED
- Wednesday, January 5, 2022 2:00pm-4:00pm (EST)
- Wednesday, January 19, 2022 9:00am-11:00am (EST)

Open Discussion Items (to be discussed at future meetings)

See attached Excel spreadsheet (CVE Board Meeting 10Nov21– Agenda and Action items.xls)

CVE Board Recordings

The CVE Board meeting recording archives are in transition to a new platform. Once the new platform is ready, the Board recordings will be readily available to CVE Board Members. Until then, to obtain a recording of a CVE Board Meeting, please reach out to CVE Program Secretariat (cve-prog-secretariat@mitre.org).