CVE Program CNA Workshop 2024 Meeting Notes

October 29-30th, 2024

Please visit the CVE Program YouTube channel for the videos of this event.

October 29, 2024: Day 1 Meeting Notes

Welcome (Alec Summers)

Rules Update (Art Manion/Kent Landfield)

- This is a living document so if there are still rules that need to be resolved, please bring them up in this workshop or via email.
- **CNA Operational Rules Revision Presentation**
    - What are the three biggest changes?
        - Right of first refusal, with time limits
            - Builds on current "most appropriate scope".
        - Technology-neutral assignments
            - Open season on cloud! And AI! Anything!
            - Informed on a significant side effort to define cloud.
        - Improved vulnerability determination and CVE ID assignment guidance
            - Clearly acknowledge that CNAs must use judgment sometimes.
    - Right of Refusal: a contractual agreement between two parties that gives one party first initial rights.
        - Rules are agnostic to the type of technology.
        - The CNA of last resort can assign if the (first) CNA declines.
        - The CNA still has discretion about what to assign for.
    - What was the process for changing the rules?
        - Core work performed in the SPWG
        - Revise, consolidate, and update glossary
        - Have an editor
    - Future process?
        - Proposed but not yet decided:
            - Markdown in a CVE GitHub repository
            - Issues, pull requests, maybe discussions
            - Periodically collect and adjudicate changes (at least once a year? As needed?)
    - CHAT QUESTION: (Rule 4.5.1.3) Does publicly disclosed include advisory publication, blog posts, etc.? Can CNAs still reserve CVEs for over 72 hours?
        - Response: Correct. CVE IDs may be reserved for a time (short or long) during disclosure coordination. Then CVE records are published when the CVE ID is made public. And any form of public release of the CVE ID means "public".
    - How are other CVE program rules affected?
        - CVE Program Glossary
            - Updated recently, more additions are likely
            - Tried to use existing definitions

                - Remove local glossary instances, update terms
            - CVE Program Policy and Procedure for Disputing a CVE Record
                - Scope/title clarification
                - Reduce friction
            - Comment: There's no program mechanism to block a CVE assignment. The closest you get is to decline writing a CVE, someone else will, then you can dispute it (assuming you still want to dispute it).
            - End of Life Vulnerability Assignment Process
                - Resolve the "Temporary CNA Rules Inconsistency"
                - CVE Program Policy and Procedure for Inactive CNAs
    - What is the "noble exception"?
        - 4.1.5
        - 4.1.5.1
        - 4.1.5.2
    - Which states can a CVE ID be in?
        - Reserved
        - Published
        - Rejected
    - What are tags?
        - Labels used to indicate defined characteristics of CVE Records
            - Exclusively-hosted-service: all known products affected by the CVE ID exist only as fully hosted services. If vulnerability affects both hosted services and on-premises products, then this tag should not be used.
            - Unsupported-when-assigned: at the time of CVE assignment, all known products affected by the CVE ID no longer receive security fixes. Products are no longer supported and considered EOL (end of life).
            - Disputed: a CVE ID assignment or CVE record content have been disputed.
    - CHAT QUESTION: how often do adversaries turn early CVEs (pre-patch) into weaponized exploits? The usual complaint about publishing early is that the vendor does not want to enable attackers.
        - Response: It becomes a subjective risk decision. It happens a lot of times and comes with the potential of early patching.
    - CHAT QUESTION: For the exclusively hosted service tag, is it used to show that the product has hosted and on-premises versions? Or is it to show that vulnerability only affects a hosted service? So, in the Word example, if the vulnerability only affects the hosted Word service and NOT the on-premises version, the CNA should mark this as exclusively hosted service right?
        - Response: If a vulnerability affected the online version only, that exclusively-hosted-service tag would apply. The tag applies to the CVE record.
        - Response: I would expect that if it's both cloud/prem, it would not get the cloud tag, at least the exclusive part of exclusively-hosted-service.

25th Anniversary (Kent Landfield)

- **25 Year Celebration Presentation**
    - **CVE Beginnings started in 1999**

        - Reasons for CVE:
            - No common naming convention for vulnerabilities.
            - Extremely labor intensive to compare output from different vendors' assessments or intrusion detection tools (IDS).
            - To relate tools with other information sources.
        - CVE was originally envisioned by Steve Christey Coley and David Mann.
    - **CVE Program Operations and Governance 1999-2016**
        - CVE Editorial Board -> MITRE -> CNAs
        - MITRE was solely responsible for virtually assigning CVEs.
        - In 2016, the CVE Board became responsible for the strategic direction, governance, operational structure, policies, and rules of the CVE Program. The Board initiated the SPWG.
    - **CVE at 25: Program Structure**
        - Federation in Action includes: 8 working groups, 2 top-level roots, 5 roots, 2 CNA-LRs, 412 CNAs, 1 ADP, and 40+ countries.
    - **Community Engagement and Federation**
        - Community engagement through CVE Working Groups and events bring valuable insights into CVE. CVE WGs are helping the program evolve supporting strategic, operational, outreach and coordination efforts.
        - CVE Record production scaled rapidly with the program's federation between 2016-2017.
    - **Evolution of CVE Data Format**
        - CVE's Record format evolved from an unstructured set of three text data elements to a rich, structured format capable of handling a large variety of data elements as needed for vulnerability management.
        - 1999 Initial Syntax – three elements CVE ID, a brief description and an external reference to relevant information.
        - 2014 – expanded CVE syntax to allow more than 9,999 CVE-OD assignments per year.
        - 2018 – piloted JSON 4.0 version to capture more vulnerability information – Pilot became production.
        - 2022 – JSON 5.0 enabled more structured data to enable better automation and integration.
    - **CVE at 25: Backbone of the Vulnerability Management Ecosystem**
        - CVE Records feed a multitude of downstream data consumers across industries, government, and academia.
    - **The Foundation for Vulnerability Prioritization**
        - CVE is the pivot point for cybersecurity risk management and prioritization.
        - Industry and researchers score and prioritize CVE records using a variety of criteria, including severity, stakeholder context, exploitability, impact, and others.
        - As the community learns more about adversary behavior and develops new methods to prioritize vulnerabilities, CVE will remain the common identifier on which to coordinate.

CVE Record Enrichment (Alec Summers)

- CVE Record Enrichment Presentation
    - What is CVE Record Enrichment?

        - CVE has become the de facto international standard for vulnerability identification.
    - Why is it important?
        - Increases the value of CVE Record.
        - More accurate, precise and timely information helps defenders and downstream customers better address risks.
        - Further positions the CVE Record as the one-stop shop for vulnerability identification.
    - Who should do CVE Record Enrichment?
        - Historically, CVE Record Enrichment has been performed by downstream consumers.
            - Enrichment was commonly informed by interpreting publicly available resources.
        - CNAs are the BEST POSITIONED to provide enrichment information.
            - Authoritative source of vulnerability information within their CNA scope
            - Closest to the products themselves
            - Have access to the most reliable source for accurate determination
    - A Look at Current Data
        - Enrichment Initiative launched in April 2024 encouraged CNAs to enrich their CVE records with CVSS and CWE at the time of disclosure.
        - CVE Program Secretariat pulls CVE data on a bi-weekly basis to track adoption throughout the CNA community.
        - CNA Enrichment Recognition List
            - Tracks CNAs that provide CVSS and CWE information 98% of the time or more within the two-week period of their last published CVE Record are added.
    - CHAT QUESTION: Can you talk about “awaiting analysis”?

CWE Usability Changes (Alec Summers)

- **An Update to CWE Usability Changes Presentation**
    - **Background**
        - In response to community feedback on the lack of usability, the CWE Program is taking action!
            - Community groups set up in response whose work has led to some tangible improvements already.
        - The CWE Program is working to address usability and understandability in further ways throughout the corpus structure and down to individual weakness language.
            - At both the micro- and macro-levels.
    - **Community Working Groups**
        - User Experience Working Group
            - Identifying areas where CWE content, rules, guidelines, and best practices must improve to better support stakeholder community and work collaboratively to fix them.
        - Root Cause Working Group
            - Established to improve and scale accurate cause mapping by better correlating CVEs with CWEs in a decentralized manner.
    - **Initial Improvements**

        - CWEs can be filtered based on specific content of interest.
        - Four default settings and customs.
        - Setting applies when navigating to different entries.
    - **CWE Usability Improvements**
        - The CWE Team continuing to categorize usability improvements in two ways.
            - Micro – how to define a weakness concisely and accurately
            - Macro – how to improve the site-wide search, navigability, and groupings of CWE information
    - **Micro CWE Updates: What's Included?**
        - CWE entry language improvements
            - Revise CWEs for more understandable language; remove redundancy.
            - Simplify CWE descriptions to use other schema elements appropriately (e.g., remove example instance, impacts, etc. from descriptions)
        - Reorder schema elements or facilitate tailoring to prioritize information (e.g., descriptions, consequences, mitigations…).
        - Visualizations: adding entries to explain topics visually
    - **Data Call: User Interviews**
        - CWE Website Recommendations vs. UX Research/Design Next Steps
    - **Improving Search – Facilitating RCM with CWE**
        - Enable interaction with CWE information vs searching it.
        - Community is developing a grounded LLM tool for improved CWE root cause mapping.
            - Building instructions and guidance available: cybersecai.github.io
        - Exploring deployment opportunities
            - CWE site, client(s) for creating/editing CVE records

CVE Services Infrastructure Update (Kris Britton)

- **CVE Services Infrastructure Update Presentation**
    - Kris explained and demonstrated how the CVE Program Goal Automation Architecture Diagram works.
    - **CVE Automation Updates in 2024**
        - Maintenance
        - CVE Record Enrichment Support
            - Authorized Data Publishing (ADP)
            - CVE Program added data
        - Ongoing Development Efforts
            - Updated CVE list search capabilities
    - **CVE Services – Maintenance**
        - Continued maintenance for CVE services and cve.org
        - CVE Record Schema updates
    - **Authorized Data Publishing (ADP)**
        - What is an Authorized Data Publisher?
            - An authorized entity with a specific scope and responsibility to enrich the context of CVE Records of already published by CVE Numbering Authorities.
        - Are there any Authorized Data Publishers?
            - CISA publishes the following:

        - Where does ADP provided data reside?
            - A new container in the CVE Record called the ADP Container ("ADP").
    - **CVE Program Container**
        - What is the CVE Program Container?
            - A special data structure that will contain additional information provided by the CVE Program about an already published vulnerability.
                - Implemented as an "ad" container
                - Container title: "CVE Program Container"
                - Assigner: "CVE"
            - Today, data in this container comprises additional references the Secretariat has added to published CVE Records
    - **Updating CVE List Search Capabilities**
        - Today's CVE List Search Capability
            - Implemented across multiple locations/methods
        - New CVE List Search Capability
            - Goal to provide a robust, consolidated search capability to search on terms/phrases across the full CVE Record
        - Status
            - Initial Operating Capability in community review/testing

CPE/purl (MegaZone/Chris Coffin)

- **CVE Program and the CVE Record Format**
    - The CVE Program has been expanding beyond a simple ID, description, and some references.
    - Federation efforts have shifted CVE Record creation to the vendors, developers, and security communities wherever possible.
    - CVE Records can store much more information than what was possible in the past.
    - The CVE Record Format (JSON Schema) defines what information can be provided and stored within a CVE Record.
- **CVE Record Format – Software/Hardware Identifiers**
    - The CVE Record Format allows CVE Record authors to include any of the following: affected/fixed product and version strings, affected/fixed collection URL and package name strings, an array of CPEs.
    - The current CVE Record Format allows CPEs to be captured as part of a CVE Record, but the CPE format semantics are insufficiently defined in the current version.
    - We need a better solution for capturing CPEs.
- **Why CPE?**
    - NIST NVD has been supplying CPEs to the community for "many years" and many tools and consumers rely on them for software identification.
    - The CISA Secure by Design pledge is pushing organizations to provide CWEs and CPEs as part of their CVE Records.
- **CVE Record Format – Enhanced CPE Support**
    - CVE Board recently approved the new CVE Record Format CPE syntax.
    - The new CPE syntax is forked from the NIST NVD CVE API v2.0 schema and is an implementation of the CPE Applicability Language.

        - The new syntax allows: CPE Identifier Names, Match Strings, and Match String Ranges to be defined and complex relations to be defined between multiple CPEs using Boolean logic.
- **New CVE Record Format Example Breakdown: applicability**
- **Future CPE Additions/Process**
    - May not be available in Vulnogram right away.
    - We will probably need to coordinate with the NIST NVD Team going forward to ensure CPE consistency with NIST NVD CPE dictionary.
        - It's possible that they can start monitoring the CPEs provided via CVE Records and update the NVD dictionary accordingly.
    - We can use the CVE Program to develop tools to help CNAs define and use CPE.
        - Potential web app to help CNAs define CPEs?
        - App could store previous CPEs and data to make it easier to generate new CPEs moving forward.
        - Could it also integrate with the current NIST NVD CPE dictionary?
- **More Identifiers Needed**
    - The CVE Record Format must support multiple product identifiers and not just CPE.
    - We may want to update CVE Record Format to allow "other" product identifier types to be defined, like other metrics.
    - Recent discussions suggest that we should target implementing PURL identifiers within the CVE Record Format as a next priority.
- **What is PURL?**
    - A software identifier format favored by many open-source communities.
    - A purl (or package URL) is an attempt to standardize existing approaches to reliably identify and locate software packages.
- **Why would someone use PURL?**
    - Reliably reference the same software package across inventory and scanning tools.
    - Allow systems/tools to collect, catalog and monitor package information such as versions, dependencies, licensing, etc. across multiple package managers.
    - Help track known vulnerabilities of a package or its dependencies, including the multiple incarnations of the same code package across different packaging systems.
    - Other kinds of analysis such as building dependency graphs of packages, etc.
- How is PURL defined?
    - A purl is a URL composed of seven components.
    - The definitions of each component were provided on-screen for further inquiry and knowledge.

Update on CVE and AI/ML/LLM (Erick Galin kin/Scott Lawler)

- **CVE AI Working Group Problem Space**
    - How does increasing adoption of artificial intelligence and machine learning impact the assignment of CVEs?
        - Does it even impact at all?
    - What is the scope of the CVE Program with respect to vulnerabilities in AI models, systems, and applications?
        - What does it mean for a model to have a vulnerability?
        - Are system-level vulnerabilities e.g. command injection introduced by models functioning as intended in scope?
    - Not all issues with AI models are in scope for CVE.

        - Define clearly what is and isn't.
- **Progress So Far**
    - Primarily administrative
        - Created charter, named a chair, established meeting cadence
    - Discussion of large language models generating vulnerable code
        - Does an LLM that generates vulnerable code merit CVE assignment to that model?
            - Models can generate both secure and insecure code.
            - May require statistical methods.
        - CVEs are for recognizing vulnerabilities and holding code providers accountable.
        - CVE IDs are not assigned for poor LLM responses.
    - CWE-1426: Improper Validation of Generative AI Output – should assignment be possible for "unintended access to reasoning"?
        - LLM providers, generally, are not specific about what they will not generate.
        - If an LLM violates an explicit or implicit security policy, it could warrant a CVE assignment.

CVE Record Hygiene and Tools (Dave Morse)

- Dave demonstrated an example of today's CVE Records. The screenshot features a CVE Record view and a JSON view.
- CNAs control enhanced data only in their CNA container.
    - ADPs provide additional data in a separate container.
    - CNAs can add other "scores" within their CNA container.
    - ADPs may defer to CNA and remove ADP provided data.
- CVE Record Management Guidelines
    - When updating existing CVE descriptions
        - Additional clarifying detail: information that enhances understanding of the vulnerability is allowed and encouraged.
        - Errors may be corrected.
        - Removing information is generally not allowed.
        - Altering information is generally not allowed.
    - Description length
        - The current temporary limit is 3999 characters. Soon, this will be modified to 4096 as specified in the new schema.
    - Preserving references is important. This is the reason the new CVE Program container was created. References added by the program are maintained in this container.
- Reasons to update CVE Records (rules 4.5.3)
    - Additional details, patches, enhanced data, etc.
    - Additional or changed references
    - Impacts of "time"
    - Splitting, merging, or rejecting (e.g., duplicate records)
    - Disputed records
- Cleaning up unused CVE IDs
    - "Reserved" CVE ID information is available via CVE Services
- CVE loves community innovation!
    - CVE encourages community members to innovate to address new CVE use cases. Any new tools or resources, bring it to a working group to share.

Day One Wrap Up (Alec Summers)

- Additional discussion was had on various other topics mentioned in the chat and Q&A feature.

October 30, 2024: Day 2 Meeting Notes

Welcome (Alec Summers)

Record Quality: Trends, Inhibitors, Requirements (Lisa Olson)

- **Growing responsibilities of CNAs in 2024**
  - What happened to heighten the need for CVE Numbering Authorities (CNAs) to enrich their CVE data?
    - The Secure by Design Pledge
    - The CVE Program Data Enrichment push has made significant jumps this year in the number of CNAs enriching the CVE data.
    - National Vulnerability Database (NVD) troubles
- **CNAs: Owning our own message**
  - Most CNAs are the experts of their CVEs
    - CVSS Scoring
    - Setting CWEs
    - CPEs?
  - There's power in group thinking.
    - It is encouraged to work together on CVSS scoring.
    - Pay attention to the 'snarky tweets' and do not be afraid to change a score after the fact if they've made a good point.
    - Join the RCM WG
    - Take the CVSS courses on FIRST.org
- **Question your Scores (we use FAQs)**
- **CVSS 3.1 vs CVSS 4.0 Poll**
  - The CVSS SIG is running a survey regarding the adoption of CVSS 4.0. Please consider adding your voice.
- **The CPE Challenge – Microsoft Efforts**
  - MRSC started publishing CPE only to CVE.org in December 2023.
  - Microsoft republished the CVEs back to 2020 to contain CPEs and discovered that the very few CNAs that were supplying CPEs were all using the standard differently.
  - The CVE Board voted to change the CPE structure in CVE.org to match the NVD structure.
  - What about the maintenance of the CPE dictionary?
- **Examples of CVEs**
  - These CPEs require no customer action to resolve.
    - 4.2.2.2: CNAs <u>should</u> publicly disclose if vulnerability has the potential to cause significant harm or requires action or risk assessment by parties other than the CNA.
  - Microsoft is disclosing cloud-based vulnerabilities that required no customer action to resolve this summer based on the change of the CNA Assignment rules (e.g., CVE-2024-38139 – Security Update Guide).
  - Crawl – Walk – Run
    - This June, Microsoft started publishing CVEs for vulnerabilities that were assessed and deemed as "critical".

Partner Membership Requirements Discussion (Tod Beardsley)

- This presentation was heavily carried out through slido.com with submissions by the participants.
- **What do the next 400 CNAs look like?**
- **What organizations would make for good CNAs?**
    - Cloud
    - Universities
    - Vendors
    - Bug Bounties
    - LATAM
    - APAC
    - OSS
    - CERTs
    - PSIRTs
    - EMEA
    - Researchers
    - And more…
- **Criteria and Expectations for new CNAs**
    - Safe-Harbor
    - Resources
    - Global
    - Collaboration
    - Commitment
- **What do you (the participants and panelists) think about new CNAs' expectations?**
    - Accuracy
    - Transparency
    - Coordination
    - Timeliness
    - Quality
    - Open to feedback
    - Learning how CVE works
- **What are undesirable behaviors of CNAs?**
    - Delays
    - Lawerly
    - NDAs
    - Deflection
    - Coverups
    - Threats
    - Lawsuits
    - Unresponsive
- **CVE Quality**
    - Writing Effective CVEs
        - Clarity
        - Specificity
        - Transparency
        - Versions/Updates
        - References
- **Inscrutable CVEs**
    - Vague

    - Evasive
    - Typos
    - Static
    - Ambiguous
    - Reserved CVEs

The Future: CVE in the Vulnerability Management Ecosystem (Panel)

- Panel speakers include Chris Coffin, Art Manion, Alec Summers, Lisa Olson, and Kent Landfield
- Questions include the program's origins, growth, future challenges, lessons learned, and opportunities for the next 25 years.
- Kent Landfield led with discussing the origin of the program and the need that developed.
    - At the start, cybersecurity was starting to become increasingly important as there were more types of intrusions in the networks and people were trying to experiment.
    - Defense in depth became the primary focus of the program. Firewalls and intrusion detection systems were no longer sufficient on their own.
- Question: Could you share an example of a particularly tough decision early on, as a writer, that the CVE program had to make? What were the challenges? What lessons were learned? What is something that we can carry forward as we continue this discussion?
    - Chris stated that the biggest turning point and controversial for the CVE program was to find better ways to produce CVEs.
    - Prior to 2016, MITRE produced all CVE records and is essentially responsible for providing all content. 2016-2017 CNAS were recruited to help which sparked controversy. Nonetheless, the CNAs were eager to help and, in the process, retained more control and more input into what went into the CVEs.
- Considering the timeframe, the modernization in CVE assignments, and the governance program rules, how have these factors influenced the program's relevance in today's security landscape?
    - Art Manion discussed a scaling issue and how the Federation had to scale the work to continue to expand. The improvement in delegating more authority to the CNAs is an enormous milestone.
- Lisa Olson advocated for the CNAs to be the frontrunners to carry out more responsibilities. The CNAs have taken over and provided very impactful contributions to the program.
    - CNAs are now the bread and butter in working together to improve the program. Between CNA involvement, the CVE Board, and the working groups there is a significant influence on the program and has since initiated changes to CVE development and improvement.
- How has the international community contributed to the program?
    - Kent Landfield: First event was held back in 2014 and was a memorable and enlightening experience to hear what they were working on and their experiences working with CVEs.

Q&A: Open Floor Discussion (Panel)

Anybody in the community was invited to not only answer questions but also ask questions. They can also present pain points, give suggestions, and comments.

Kent spoke on the misrepresentation move away from working with NVD and working with the NIST and how it has not benefited the program. The Board has decided to create a new position called an ‘organizational liaison’. NIST was invited to be one of the first to hold that position.

CHAT QUESTION: How can the CVE Program encourage more participation from underrepresented regions or sectors or industries, such as smaller companies, nonprofits, academic institutions, etc.? What are some of the things that we could do?

- Response: Even with all the current rules and processes, there are gaps in CVE coverage. There are publicly disclosed vulnerabilities floating around and they are missing the CVEID. So maybe a small, maybe not a small scale, but an immediate term sort of thing would be to try to figure out ways to more proactively just increase the known existing coverage issue gaps.
- Response: In some respects, getting to the right people who we can then explain the value of their industries, their technology bases, because everything is using technology software now.

CHAT QUESTION. Software vendors are regularly asked about vulnerabilities detected in 3rd party libraries that we could make use of in our code. What are the panel's thoughts?

- Response: We have a lot of third-party open-source stuff in our products, and we often publish security advisories for 3rd party CVEs that affect their products or don't affect their products. There is currently no good way to feed that into the CVE program so that it's consumable from central location. You'd have to go to every vendor. A solution in favor is where CNA could contribute their scope would be limited to them as ACNA.
- Response: There has been additional discussion on ACNA as ADP and adding extra information about what products they have that are affected by the upstream.

The shift of CNAs involved sparked a lot of discussions on how the program would progress and the value that their insight would bring. Several CNAs spoke on the shift and getting it to translate into vendors, software regulators and the industry itself.

Panelists also discussed how to grow within the program which referenced some of the challenges that were discussed earlier in the workshop.