CVE Program CNA Workshop 2024 Session Summaries

October 29-30th, 2024

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

This document provides a summary of the discussions, presentations, and key takeaways from the workshop. Participants included industry experts who shared insights on various topics crucial to the ongoing development and enhancement of the CVE Program.

Day One Overview

The **CVE Workshop** held on October 29, 2024, covered several key topics:

1. **CNA Operational Rules Update**: Art Manion discussed significant changes to the CNA Operational Rules, including the right of first refusal with time limits, technology-neutral assignments, and an open approach to cloud and AI. He emphasized the importance of judgment in vulnerability determination and CVE ID assignment, and addressed updates to the CVE Program Glossary, policies for disputing a CVE record, and the end-of-life vulnerability assignment process.
2. **25th Anniversary of the CVE Program**: Kent Landfield commemorated the 25th anniversary of the CVE program, highlighting its evolution from a simple naming convention for vulnerabilities to a sophisticated system managed by the CVE Board. The program now includes multiple working groups and spans over forty countries.
3. **CVE Record Enrichment**: Alec Summers presented on the importance of enhancing CVE Records to provide more accurate, precise, and timely information. An Enrichment Initiative launched in April 2024 encourages CNAs to include CVSS and CWE information at the time of disclosure.
4. **CWE Usability Changes**: Alec Summers also discussed enhancements to the CWE Program based on community feedback. Improvements include better filtering options, refined language, simplified descriptions, and enhanced search functionality.
5. **CVE Service Infrastructure**: Kris Britton provided updates on the CVE Services Infrastructure, highlighting advancements in automation, ongoing development efforts, and support for CVE Record Enrichment.
6. **CPE/PURL**: MZ MegaZone and Chris Coffin discussed the evolution of the CVE Record Format, focusing on the inclusion and enhancement of software and hardware identifiers like CPE and PURL. The new format supports detailed CPE identifiers and the potential integration of PURL identifiers.
7. **CVE and AI/ML/LLM**: Erick Galinkin explored the impact of artificial intelligence and machine learning on CVE assignment, addressing the challenges of assigning CVEs to large language models (LLMs) that generate vulnerable code.
8. **CVE Record Hygiene and Tools**: Dave Morse emphasized the importance of updating existing CVE descriptions with additional details to enhance understanding of vulnerabilities. He also highlighted the need for cleaning up unused Reserved CVE IDs and encouraged community innovation in processes and tooling.

These summaries reflect the ongoing efforts to enhance the CVE program's infrastructure, usability, and overall effectiveness in managing and disseminating vulnerability information.

CNA Operational Rules Update (Art Manion)

Art Manion provided an update on the CNA Operational Rules, highlighting significant changes such as the right of first refusal with time limits, technology-neutral assignments, and an open approach to cloud and AI. It emphasizes the importance of judgment in vulnerability determination and CVE ID assignment, outlines the revision process, and discusses future procedural proposals. Additionally, it addresses updates to the CVE Program Glossary, policies for disputing a CVE record, the end-of-life vulnerability assignment process, and policies for inactive CNAs. It also explains CVE ID states and the use of tags to indicate characteristics of CVE records.

1. **Right of First Refusal with Time Limits**: This change builds on the current "most appropriate scope" and introduces a contractual agreement between two parties that gives one party the initial rights within a specified time frame.
2. **Technology-Neutral Assignments**: The rules are now agnostic to the type of technology, allowing for open assignments on cloud, AI, and other technologies. This includes improved guidance for vulnerability determination and CVE ID assignment.
3. **Revision Process and Future Proposals**: The revision process involved the SPWG, updating the glossary, and considering future processes using a CVE GitHub repository. This includes addressing the impact on other CVE program rules, such as dispute resolution and handling inactive CNAs.

25th Anniversary (Kent Landfield)

The presentation commemorates the 25th anniversary of the Common Vulnerabilities and Exposures (CVE) program, initiated in 1999 by Steve Christey Coley and David Mann. Initially, there was no standardized naming convention for vulnerabilities, making it labor-intensive to compare outputs from various tools. From 1999 to 2016, MITRE managed CVE assignments, but in 2016, the CVE Board assumed control, setting strategic directions and policies. The program's structure now includes multiple working groups, roots, CNAs, and spans over 40 countries. The CVE record format has evolved significantly, from a simple three-element structure to a sophisticated JSON format, enhancing automation and integration. CVE records are crucial for vulnerability management and prioritization across industries, governments, and academia.

1. **Origins and Purpose**: The CVE (Common Vulnerabilities and Exposures) program was initiated in 1999 by Steve Christey Coley and David Mann to address the lack of a common naming convention for vulnerabilities, which made it labor-intensive to compare outputs from different vendors' tools.
2. **Governance and Evolution**: From 1999 to 2016, MITRE was solely responsible for assigning CVEs. In 2016, the CVE Board took over the strategic direction, governance, and operational structure of the program. The program now includes multiple working groups and a global community of 412 CNAs across 40+ countries.
3. **Data Format Advancements**: The CVE record format has evolved from a simple three-element structure to a sophisticated JSON 5.0 format, enabling better automation and integration. This evolution has significantly enhanced the program's ability to manage and prioritize vulnerabilities.

CVE Record Enrichment (Alec Summers)

The presentation on CVE Record Enrichment by Alec Summers outlines the importance of enhancing CVE Records to increase their value by providing more accurate, precise, and timely information. This enrichment aids defenders and downstream customers in better addressing risks and solidifies the CVE Record as the primary source for vulnerability identification. Historically, enrichment was performed by downstream consumers using publicly available resources, but CNAs are now recognized as the best positioned to provide this information due to their authoritative knowledge and proximity to the products. An Enrichment Initiative launched in April 2024 encourages CNAs to include CVSS and CWE information at the time of disclosure, with the CVE Program Secretariat tracking adoption bi-weekly and recognizing CNAs that consistently provide this information.

1. **Importance of CVE Record Enrichment**: Enhancing CVE Records with accurate, precise, and timely information increases their value, aids defenders and downstream customers in addressing risks, and solidifies the CVE Record as the primary source for vulnerability identification.
2. **Role of CNAs**: Historically, downstream consumers performed CVE Record Enrichment using publicly available resources. However, CNAs (CVE Numbering Authorities) are now recognized as the best positioned to provide this information due to their authoritative knowledge and proximity to the products.
3. **Enrichment Initiative**: Launched in April 2024, this initiative encourages CNAs to enrich their CVE records with CVSS and CWE information at the time of disclosure. The CVE Program Secretariat tracks adoption bi-weekly and recognizes CNAs that consistently provide this information.

CWE Usability Changes (Alec Summers)

The CWE Program is enhancing usability in response to community feedback. Community groups have been established, leading to initial improvements. The program aims to improve both the corpus structure and individual weakness language at micro and macro levels. Two working groups, User Experience and Root Cause, focus on improving content and cause mapping, respectively. Initial improvements include better filtering of CWEs. Micro-level updates involve refining language and simplifying descriptions, while macro-level updates enhance search and navigability. Future developments include improving search functionality and developing a tool for better root cause mapping.

1. **Community Feedback and Initial Improvements**: The CWE Program is enhancing usability based on community feedback. Community working groups have been established, leading to initial improvements such as better filtering options for CWEs.
2. **Micro and Macro-Level Updates**: The program aims to improve both the corpus structure and individual weakness language at micro and macro levels. Micro-level updates involve refining CWE language and simplifying descriptions, while macro-level updates enhance search functionality and site navigability.
3. **Future Developments**: Future enhancements include visual aids, user interviews, and the development of a grounded LLM tool for better root cause mapping.

CVE Service Infrastructure (Kris Britton)

The presentation provided an update on the CVE Services Infrastructure, presented by Kris Britton. It covered several key areas:

1. **CVE Automation Updates in 2024**: Kris Britton explained and demonstrated the CVE Program Goal Automation Architecture Diagram, highlighting the advancements in automation for the CVE program.
2. **Maintenance and Ongoing Development Efforts**: The presentation emphasizes the importance of continued maintenance for CVE services and the cve.org website. It also discusses ongoing development efforts to enhance the CVE infrastructure.
3. **CVE Record Enrichment Support**: The presentation outlines the support for CVE Record Enrichment, which aims to provide more accurate and timely information for CVE records4.
4. **Authorized Data Publishing (ADP)**: The concept of Authorized Data Publishers is introduced, describing their role in enriching the context of CVE Records already published by CVE Numbering Authorities. The presentation also explains where ADP-provided data resides within the CVE Record.
5. **CVE Program Container**: A special data structure called the CVE Program Container is described, which contains additional information provided by the CVE Program about already published vulnerabilities89.
6. **Updated CVE List Search Capabilities**: The presentation discusses the improvements in CVE list search capabilities, aiming to provide a robust and consolidated search functionality across the full CVE Record.

These updates reflect the ongoing efforts to enhance the CVE program's infrastructure, ensuring it remains effective and efficient in managing and disseminating vulnerability information.

CPE/PURL (MegaZone/Chris Coffin)

MegaZone and Chris Coffin discuss the evolution and expansion of the CVE Program, particularly focusing on the CVE Record Format and its support for software and hardware identifiers. The CVE Program has evolved from providing simple IDs and descriptions to incorporating more comprehensive information, with the creation of CVE Records now being delegated to vendors, developers, and security communities. The new CVE Record Format includes an improved CPE syntax derived from the NIST NVD CVE API v2.0 schema, allowing for detailed CPE identifiers, match strings, and complex relations between multiple CPEs using Boolean logic. Additionally, The presentation highlights the potential integration of PURL identifiers within the CVE Record Format, which are favored by open-source communities for reliably identifying and tracking software packages across various tools and systems.

The presentation discussed the evolution of the CVE Record Format, particularly focusing on the inclusion and enhancement of software and hardware identifiers like CPE and PURL.

- **Expansion of CVE Program**: The CVE Program has evolved to include more detailed information beyond simple IDs and descriptions, with record creation now involving vendors, developers, and security communities.
- **Enhanced CPE Support**: The CVE Record Format now supports an enhanced CPE syntax for better software identification, incorporating Boolean logic to define complex relationships between CPEs.

- **Introduction of PURL**: The presentation suggests the future inclusion of PURL, a software identifier format favored by open-source communities, to standardize the identification and tracking of software packages.

Update on CVE and AI/ML/LLM (Erick Galinkin)

Erick Galinkin provides an update on the CVE and AI/ML/LLM initiatives. The presentation explores the impact of artificial intelligence and machine learning on the assignment of CVEs, questioning whether vulnerabilities in AI models, systems, and applications fall within the CVE Program's scope. The presentation highlights the administrative progress made so far, including the creation of a charter, the appointment of a chair, and the establishment of a meeting cadence. It also discusses the challenges of assigning CVEs to large language models (LLMs) that generate vulnerable code, emphasizing that CVEs are meant for recognizing vulnerabilities and holding code providers accountable. The presentation concludes by addressing the potential for CVE assignments when an LLM violates explicit or implicit security policies.

1. **Impact of AI/ML on CVE Assignment**: The presentation explores how the increasing adoption of artificial intelligence and machine learning affects the assignment of CVEs. It questions whether vulnerabilities in AI models, systems, and applications fall within the CVE Program's scope.
2. **Administrative Progress**: Significant administrative progress has been made, including the creation of a charter, the appointment of a chair, and the establishment of a meeting cadence.
3. **Challenges with Large Language Models**: The presentation discusses the challenges of assigning CVEs to large language models (LLMs) that generate vulnerable code. It emphasizes that CVEs are meant for recognizing vulnerabilities and holding code providers accountable.

CVE Record Hygiene and Tools (Dave Morse)

Dave Morse presented on CVE Record Hygiene and Tools, demonstrating today's CVE Records with examples of both CVE Record and JSON views. He explained that CNAs control enhanced data within their CNA container, while ADPs provide additional data and may defer to CNAs by removing ADP-provided data. CNAs can also add other scores. The presentation covered CVE Record Management Guidelines, emphasizing the importance of updating existing CVE descriptions with additional clarifying details to enhance understanding of vulnerabilities. Errors, removing or altering information, and description length were discussed, with a temporary limit of 3999 characters soon to be updated to 4000. The guidelines also included preserving references, reasons to update CVE Records, impacts of time, and handling disputed records. Additionally, the presentation highlighted the importance of cleaning up unused CVE IDs and encouraged community innovation, inviting members to share new tools or resources with working groups.

1. **CVE Record Hygiene and Tools**: Dave Morse demonstrated examples of current CVE Records, highlighting both the CVE Record view and the JSON view. He explained that CNAs control enhanced data within their CNA container, while ADPs provide additional data and may defer to CNAs by removing ADP-provided data. CNAs can also add other scores.
2. **CVE Record Management Guidelines**: The guidelines emphasize the importance of updating existing CVE descriptions with additional clarifying details to enhance understanding of vulnerabilities. They also cover errors, removing or altering information, and description length, with a temporary limit of 3999 characters soon to be updated to

4000. The guidelines include preserving references, reasons to update CVE Records, impacts of time, and handling disputed records.

3. **Community Innovation and Cleanup**: The presentation highlighted the importance of cleaning up unused CVE IDs and encouraged community innovation. Members are invited to share new tools or resources with working groups to address new CVE use cases.

Day Two Overview

The **CVE Workshop** held on October 30, 2024, covered several key topics:

1. **Growing Responsibilities of CNAs in 2024**: The presentation highlighted the increasing responsibilities of CVE Numbering Authorities (CNAs) and the importance of enriching CVE data to improve record quality.
2. **CVE Program Data Enrichment and Secure by Design Pledge**: Significant progress has been made this year in the CVE Program Data Enrichment push, with more CNAs enriching their CVE data. The Secure by Design Pledge was also discussed as a key initiative.
3. **Collaboration and Transparency**: The presentation emphasized the need for CNAs to own their messaging, collaborate on CVSS scoring, and be open to feedback, even from social media. It also addressed issues with the National Vulnerability Database (NVD) and the disclosure of cloud-based vulnerabilities.
4. **Future of CNAs**: The presentation explored the characteristics and expectations for the next 400 CNAs, identifying potential organizations such as cloud providers, universities, vendors, bug bounty programs, and regional entities like LATAM, APAC, and EMEA. It emphasized the importance of criteria such as accuracy, transparency, coordination, timeliness, and quality for new CNAs.
5. **Undesirable Behaviors and Effective CVE Writing**: The presentation addressed undesirable behaviors of CNAs, including delays, legalistic approaches, non-disclosure agreements (NDAs), deflection, coverups, threats, lawsuits, and unresponsiveness. It also highlighted the importance of writing effective CVEs with clarity, specificity, transparency, and proper references.
6. **Panel Discussion Insights**: The panel featured speakers Chris Coffin, Art Manion, Alec Summers, Lisa Olson, and Kent Landfield. They discussed the program's origins, improved CVE generation methods, scaling challenges, and the significance of the first international event in 2014.

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

The presentation covered several key topics related to the responsibilities and challenges faced by CVE Numbering Authorities (CNAs) in 2024. It highlighted the growing responsibilities of CNAs and the importance of enriching CVE data to improve record quality. The Secure by Design Pledge and the CVE Program Data Enrichment push were discussed, emphasizing the significant progress made this year. The presentation also addressed issues with the National Vulnerability Database (NVD) and the need for CNAs to own their messaging. It encouraged collaboration on CVSS scoring and the importance of being open to feedback, even from social media. Additionally, the presentation touched on the CPE Challenge and Microsoft's efforts to publish CPEs, as well as the changes in CNA Assignment rules and the disclosure of cloud-based vulnerabilities. Overall, the presentation underscored the importance of collaboration, continuous improvement, and transparency in the CVE process.

1. **Growing Responsibilities of CNAs in 2024**: The presentation highlighted the increasing responsibilities of CVE Numbering Authorities (CNAs) and the importance of enriching CVE data to improve record quality.
2. **CVE Program Data Enrichment and Secure by Design Pledge**: Significant progress has been made this year in the CVE Program Data Enrichment push, with more CNAs enriching their CVE data. The Secure by Design Pledge was also discussed as a key initiative.
3. **Collaboration and Transparency**: The presentation emphasized the need for CNAs to own their messaging, collaborate on CVSS scoring, and be open to feedback, even from social

media. It also addressed issues with the National Vulnerability Database (NVD) and the disclosure of cloud-based vulnerabilities.

Partner Membership Requirements Discussion (Tod Beardsley)

The presentation, primarily conducted through slido.com with participant submissions, focused on the future of CVE Numbering Authorities (CNAs). It explored the characteristics and expectations for the next 400 CNAs, identifying potential organizations such as cloud providers, universities, vendors, bug bounty programs, and regional entities like LATAM, APAC, and EMEA. The discussion emphasized the importance of criteria such as accuracy, transparency, coordination, timeliness, and quality for new CNAs. It also highlighted the need for CNAs to be open to feedback and to understand how CVE works. Additionally, the presentation addressed undesirable behaviors of CNAs, including delays, legalistic approaches, non-disclosure agreements (NDAs), deflection, coverups, threats, lawsuits, and unresponsiveness. The importance of writing effective CVEs with clarity, specificity, transparency, and proper references was also underscored.

Sure, here are the three main points from the presentation notes:

1. **Characteristics and Expectations of** CNAs: The presentation discussed the characteristics and expectations for the next 400 CVE Numbering Authorities (CNAs), highlighting potential organizations such as cloud providers, universities, vendors, bug bounty programs, and regional entities like LATAM, APAC, and EMEA.
2. **Important Criteria for CNAs**: It emphasized the importance of criteria such as accuracy, transparency, coordination, timeliness, and quality for new CNAs, as well as the need for CNAs to be open to feedback and to understand how CVE works.
3. **CVE Writing and Behaviors for CNAs:** The presentation addressed undesirable behaviors of CNAs, including delays, legalistic approaches, non-disclosure agreements (NDAs), deflection, coverups, threats, lawsuits, and unresponsiveness. It also highlighted the importance of writing effective CVEs with clarity, specificity, transparency, and proper references

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

The panel featured speakers Chris Coffin, Art Manion, Alec Summers, Lisa Olson, and Kent Landfield. Kent Landfield initiated the discussion by outlining the program's origins and the necessity for its development. Chris Coffin provided insights into improved methods for generating CVEs and establishing best practices. Art Manion addressed the challenge of scaling operations, noting significant progress through greater delegation to CNAs. Lisa Olson advocated for CNAs to assume more responsibilities, emphasizing their substantial contributions. Kent Landfield also highlighted the significance of the first international event in 2014, which showcased the global community's efforts with CVEs.

Program Growth: Opportunities and Challenges (Panel)

The workshop panel discusses on the growth of the CVE Program, highlighting opportunities and challenges.

Community Engagement and Representation: The panel emphasized the importance of community involvement, including encouraging participation from underrepresented regions and sectors, and addressing gaps in CVE coverage by reaching the right people and explaining the value of their industries and technologies.12

Handling Third-Party Vulnerabilities: Panelists discussed the challenges of managing vulnerabilities in third-party libraries, suggesting the need for a centralized way to handle security advisories from various vendors and the role of CNAs in contributing to the program.

The shift of CNAs being 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.

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