CNA Fall Technical Workshop Meeting Summaries

October 22-23, 2025

The 2025 CNA Fall Technical Workshop brought together more than 250 participants to align on improving the accuracy, consistency, and usability of CVE Records and to shape the program's future direction. Across two days of panels, technical deep dives, and guided listening sessions, attendees emphasized the need for stronger data quality, clearer schema requirements, expanded machine-readability, and better support for CNAs and consumers.

Key discussions centered on SSVC integration, CWE root cause mapping, CVSS v4.0 updates, PURL and CPE usage, VEX/CSAF adoption, the Supplier ADP Pilot, and modernization of tooling and validation. New initiatives, including the Reference Archive Pilot, Record Format roadmap updates, and the formation of the Consumer Working Group, demonstrated the program's commitment to improving transparency, automation, and long-term reliability.

This document summarizes the key discussions, decisions, and insights shared during the 2025 CNA Fall Technical Workshop. It provides a high-level overview of major themes and program developments, with detailed session notes available in the sections that follow. Raw notes are included for reference here.

Day One Overview

The first day of the **CNA Fall Technical Workshop,** held on October 22, 2025, convened CVE Numbering Authorities (CNAs) to engage in panel discussions, surveys, feedback and reporting sessions, and informational presentations.

These sessions explored several key topics:

1. **CVE Data Quality**: The CVE Program relies on the production and maintenance of high-quality CVE Records. Chris Coffin, Jerry Gamblin, and Jay Jacobs led a panel discussion evaluating what constitutes data's completeness, utility, and quality, and how data collected in the record can maximize value provided to CNAs.
2. **Community Feedback**: Speakers Jen Ellis and Lisa Olson moderated a listening session on the status and ideal future state of the CVE Program. Participants expressed interest in prioritizing data quality and accuracy, emphasizing that certain fields should be required and parameters for their use should be made clear to all maintainers.
3. **Adoption of SSVC in CVE Records**: In a session guided by Vijay Sarvepalli, participants discussed SSVC data, its impact on CVE Records, and ways to present information to the public through decision points and decision trees. Incorporating SSVC data can enhance prioritization and decision-making for suppliers, deployers, and coordinators.
4. **Mapping CWE Root Causes in CVE Records**: As part of the ongoing effort to ensure the CVE Program provides value to the broader community, Steve Christey Coley and Connor

Mullaly presented on a recent initiative to map CVEs to CWEs. Quickly and effectively mapping CVEs to CWEs would build consumer trust and improve both internal and external (community) weakness and trend analyses.

5. **CVSS Version 4.0**: In a session on updates made in the transition from CVSS 3.1 to 4.0, Pete Allor and Nick Leali explored the expected changes, including to data sets and boundaries. The updates will improve how consumers make informed decisions through context and accuracy.
6. **CPE and PURL in CVE Records**: Participants explored the distinctions between Package URLs (PURL) and Common Platform Enumeration (CPE) in a session led by Andrew Lilley Brinker. PURLs and CPEs are complementary and will both appear in future records, as PURLs will be allowable with the release of the 5.2.0 CVE Record Format.

These summaries reflect the ongoing efforts to enhance the CVE program's infrastructure, usability, and overall effectiveness in managing and disseminating vulnerability information. The workshop was well attended, with 197 attendees on Day One, representing 112 CNAs.

Welcome & Kickoff (Alicia Mink)

Alicia Mink of MITRE, who leads CNA onboarding and recruitment for the MITRE Top-Level Root, provided introductory remarks, previewing the agenda and welcoming the first group of presenters. Alicia also thanked participants for their continued dedication to the CVE Program's mission. The CVE Program will collect feedback in a survey (below). MITRE will also provide session slides and recordings to attendees.

Links

- Fall Technical Workshop: Day 1 (Teams Recording)
- Fall Technical Workshop: Day 2 (Teams Recording)
- Post-Session Survey (available for two weeks post-session)

Completeness, Quality, and Utility (Panel Discussion)

Chris Coffin of MITRE, co-chair of the Quality Working Group and CVE Board member, Jay Jacobs of Empirical Security, and Jerry Gamblin, principal engineer at Cisco and the author of the CNA scorecard site, moderated a panel discussion on the completeness, quality, and utility of CVE Records in the schema. In the past year, 46,959 CVE Records have been published. The CVE Program relies on the contributions of its CNA partners (currently 480) to maintain the momentum of the program. Panelists and audience members discussed which aspects of CVE Records are most valuable to downstream users, helping inform which information should be captured in records.

1. **Completeness Versus Quality**: Jay Jacobs explained that completeness refers to all required fields being filled in in a CVE Record, while quality is about the usefulness of the information for decision-making and action. Jerry Gamblin agreed, emphasizing that

completeness is binary, but quality is context-dependent and should be driven by the needs of downstream consumers.

2. **CNA Scorecard**: Jerry Gamblin described the CNA Scorecard tool, which tracks the completeness of CVE Records across CNAs, noting that over 85% of CNAs provide full CVSS scores and CWE data, but software identifiers and patch arrays lag. He encouraged CNAs to improve patch data inclusion for better downstream automation. Jerry invited participants to contact him to discuss the scorecard.
    a. He encouraged the audience to reach out: jerry.gamblin@gmail.com.
    b. The CNA Scorecard is available here: https://cnascorecard.org/.
3. **Complexity of Schema:** Jay highlighted that the CVE schema allows multiple valid locations for software identification, complicating data extraction and quality assessment. The schema in its present state may be too complex to navigate intuitively. At present, roughly 75% of records discussed were under 25% utilized. It may be beneficial to eliminate features such as taxonomy mappings to make the schema more user-friendly and to improve record quality. The National Vulnerability Database (NVD) offers an example of a simpler record that directs users to other sources of specialized data outside of the schema. Jay also advocated for schema improvements and more validation to ensure consistent, high-quality data entry.
    a. **Quality**: While panelists agreed that quality is essential for the success of the CVE Program, they disagreed on how to define, assign responsibility for achieving, and maintain high-quality records. It may be beneficial to consider the accuracy, completeness, timeliness, and usefulness of records as subsets of their quality. While they are interrelated, correctness and quality should be measured independently.
    b. **Quality Improvement Recommendations**: Panelists recommended that the CVE Program focus on correctness through validation, making key fields like CWE and CVSS mandatory, and improving the schema to support machine-readable, structured data. They also stressed the need for ongoing engagement with consumers to refine quality standards.
    c. **Utility for Stakeholders**: Measuring utility will vary by stakeholder, such as pen testers, vulnerability managers, and patching teams. Actionable data like patch information is often missing, and that utility may be better defined by the top stakeholder tasks and supported by relevant data elements.
    d. **CNAs' Roles**: CNAs should understand their customers' needs, which will influence how quality is defined and the kind of data that will be required for records.
4. **Challenges with Accuracy and Delivering Value**: Jay recommended that, to improve record quality, descriptions should include fields with a minimum required input. Currently, most records contain open text fields, which cause variations that prevent users from taking a standardized approach to assessing records. By moving data into required fields, descriptions would be more standardized and easier to parse.
5. **Improving Quality and Utility**: The CVE Program and the broader community should work together to assess what quality means for different stakeholders. To advance the program

for everyone, records need to be as complete and correct as possible. Some aspects of quality will be up to the community to decide. The Program can provide a venue for the standardization of consistency.

6. **Future of CVE Records:** Any opportunity to encourage and/or require more validation will improve the overall value of records. Data should also be incorporated into clients such as Vulnogram consistently to make it available to a broader audience.

Chat Links

- https://cwe.mitre.org/top25/
- https://www.cve.org/Media/News/item/news/2025/07/01/New-CVE-Consumer-WG
- https://cnascorecard.org/scoring.html
- https://cveawg.mitre.org/api/cve/CVE-2025-36128
- https://github.com/CVEProject/cve-schema/blob/a29f28e5d48383cc5e179f9c6655ac49e8ffe1f9/schema/docs/CVE_Record_Format_bundled.json#L59
- https://cveproject.github.io/cve-schema/schema/docs/#oneOf_i0_references_patch

Guided Listening #1 (Jen Ellis & Lisa Olson)

Guest speakers Jen Ellis of NextJen Security and Lisa Olson of Microsoft, both CVE Board members, guided the group in a listening session, providing a forum for discussion and interaction. Participants provided feedback on the state of the CVE Program, the value it currently provides versus what its ideal state could be.

1. **Most Significant Problems Facing CVE**: Respondents shared that the most significant issues the CVE Program faces in order of importance are data quality and accuracy, funding, governance, technical modernization, fragmentation, transparency, and CVE counting rules.
2. **Data Challenges**: Ideally, CVE Records should be more easily machine-readable. Users also requested that CVE Records connect to features of their products such as SBOMs. Data challenges in particular lie in the "affected" field, which may be the most critical yet most misunderstood and is used inconsistently. CVE Records may leave many questions unanswered or can be open to interpretation due in large part to open entry fields. In addition, the current status quo makes it difficult to spread feedback on records to the appropriate distributions, such as curl or Kernel. For updated records to be useful, changes must reach the original reporter; but as projects fork into various branches, it becomes more difficult to manage records and their impact. It was recommended to initiate updates with the impacted original product at the CNA level.
3. **CVE Publication and Management**: Participants felt strongly that the current approach to data validation is insufficient. Participants also suggested implementing more mandatory fields and mechanisms to push CVEs back to CNAs to ensure records are clearer and more useful. Many participants rely on tools such as Vulnogram to publish CVE Records. When asked what types of information should be required for every CVE Record, they ranked

them in the following order: CVE ID, affected systems, description, severity, CWE linking, links to advisories, date of public disclosure, mitigation guidance, and confirmation of exploitation. The discussion was punctuated by the necessity of utility.

4. **Community Engagement**: Without a formalized method to collect and distribute feedback to the relevant parties, the quality of data suffers. Establishing a feedback-sharing structure that directs comments and responses to the appropriate CNAs will improve data quality and record management. When asked how the CVE Program can better support CNAs, respondents felt strongly that the Program should provide better guidance on what should be included in each field.

Chat Links

- https://github.com/callumlocke/json-formatter (To improve JSON readability)
- https://www.cve.org/Resources/General/Key-Details-Phrasing.pdf

SSVC – Feature Branch, More Formal Structure, New Version/Schema (Vijay Sarvepalli)

Vijay Sarvepalli, a Principal Architect at Carnegie Mellon University's Software Engineering Institute, joined the CNA Technical Workshop to present information regarding the benefits of adding Stakeholder-Specific Vulnerability Categorization (SSVC) Data into CVE Records. SSVC was created in 2019 to provide the cyber community with a vulnerability analysis methodology adaptive to stakeholders. He explained that through SSVC data, critical information can be shared within the metrics section of CVEs, to provide needed context to published vulnerabilities.

1. **SSVC Decision Points and Trees:** Vijay outlined SSVC Decision Points and Trees as models that guide stakeholders (e.g., Suppliers, Deployers, Coordinators) through the process of determining outcomes for a cybersecurity vulnerability, including its potential for exploitation, automation, and technical impact.
2. **SSVC Explorer and Calculation Tool:** Vijay gave a demonstration on how to use the SSVC Explorer and Calculator, which provides interactive insight into SSVC deployment and usage. Through the platforms, stakeholders can also create their own decision trees and decision points.
3. **Benefit to the Public:** Vijay explained that the public would benefit from simple methods of displaying SSVC Data in CVE Records because it would give context and reasoning behind the decisions made (e.g., patch timing, level of human impact) for classifying or acting on cybersecurity vulnerabilities.

Chat Links

- https://api.democert.org/ssvc/
- https://github.com/CVEProject/cve-schema/pull/460
- https://certcc.github.io/SSVC/

- https://github.com/FIRSTdotorg/cvss-resources
- https://pypi.org/project/certcc-ssvc/
- https://api.democert.org/ssvc/
- https://github.com/CVEProject/cve-schema/pull/460
- https://certcc.github.io/SSVC/

Effectively Mapping CVEs to CWEs (Steve Christey Coley & Connor Mullaly)

Connor Mullaly of MITRE, chair of the CWE Root Cause Mapping Working Group (RCM WG), and Steve Christey Coley of MITRE, CWE Technical Lead, introduced an ongoing initiative to improve how CVEs are mapped to CWEs to identify the root cause of real-world vulnerabilities. Identifying the root cause would provide CNAs and other developers with the tools to understand how a vulnerability was created and the most appropriate method for addressing it. The RCM WG is currently developing guidance materials and a root cause mapping AI-based tool to assist in the mapping process, providing stakeholders with additional confidence in CVE reporting.

1. **Root Cause Analysis:** Connor outlined the difference between impact and root cause by differentiating that impact is a common consequence of dozens of CWEs, while a root cause emphasizes the aspects of why something happened. The RCM WG believes that CNAs are best positioned to examine root causes through precise and accurate CWE Mapping.
2. **Mapping CVEs to CWEs:** Connor explained the various benefits of Mapping to CWEs, including improving consumer trust through mitigating vulnerabilities at the root cause rather than just the symptoms, enabling accurate trend analysis of weaknesses throughout the industry, and providing context to what mistakes developers are most commonly making. To conduct the mapping, CNAs would identify the weakness, technical impact, and prerequisite to identify the permissible CWE Mapping Usage Label. This will mitigate the current issue of CNAs using general CWE Mapping Usage Labels that do not provide enough context for accurate mapping.
3. **Potential Risk:** Connor acknowledged, and the workshop participants discussed, that CWE Mapping could lead to attackers obtaining information that would assist them in exploiting systems.
4. **LLM Tool:** The RCM WG is developing an LLM tool to aid in Root Cause Mapping. This would speed up the mapping process as it will offer Batch Assignments, Singular CVE analysis, and a CWE ChatBot for interactive help.

Goods and Bads – CVSS 3.1 vs. CVSS 4.0 (Pete Allor & Nick Leali)

Presenters Pete Allor of the CVE Board and Nick Leali of Cisco outlined the key updates of CVSS Version 4.0. The new features include supplemental metrics for CVEs which provide consumer organizations with updated Base scores and provide accurate calculations that can better inform decision-making. In addition to updating the database, there will be a focus on creating education

materials for consumer organizations to provide them with some best practices for reviewing CVEs and leveraging the data within them to evaluate risks and potential threats to systems.

1. **CVSS 3.1:** CVSS v3.1 has been a standard for over a decade and provides predictable math outcomes through well-supported tooling.
2. **CVSS 4.0:** The 4.0 version is not a drop-in replacement for version 3.1. Rather, the new version will have changes in data sets and boundaries, and overall, it introduces new math that incorporates additional properties, such as threat and environmental. The updates included will assist consumers in making more informed assessments/decisions through context and accuracy.
3. **Education on Base Score:** Currently, consumer organizations are using the simple Base score the original CNA originally reported instead of adding complementary information, such as SSVC. Pete recommended emphasizing Base score education to address this problem. There was consensus among workshop participants that this is an issue to address, and Nick Leali revealed that a guide will be released soon to consumer organizations .

Chat Links

- https://cwe.mitre.org/community/submissions/overview.html
- https://github.com/FIRSTdotorg/cvss-resources

Software ID: CPE and PURL (Andrew Lilley Brinker)

Andrew Lilley Brinker of MITRE kicked off a discussion on the capabilities and benefits of adding Package URLs (PURLs) data to new and existing CVEs, which will be available through the release of the 5.2.0 CVE Record Format. PURL is a field included in CVE reporting that can provide context surrounding a system's package to streamline categories and enhance automation.

1. **PURLs***:* A PURL is a specification for packages found on package hosts supported in CVE Records. It is intended to make automated applicability decisions for open-source software easier for CVE consumers through providing additional details. Their use is optional, they must be accompanied by an existing identifier format, and they cannot contain a version. In contrast to the current free form fields, the benefit of PURL is that the specification aspect enables ease with cross-referencing by streamlining already existing data into more specific categories.
2. **CPEs vs PURL:** While CPEs are best for commercial software, PURLs are best for open-source systems. They are, however, complementary.
3. **PURL Application:** PURL will be available along with the release of the 5.2.0 CVE Record Format. To utilize PURL, add a "packageURL" field to the objects in the "affected" array. If a commercial product is not in the public domain, then a generic type within PURL (e.g., URL, additional metadata) should be used. While the generic type is available, it is encouraged for users to assign a more specific category to CVEs for ease with pattern detection and provide deeper context.

Chat Links

- https://github.com/package-url/purl-spec
- https://fossa.com/blog/understanding-purl-specification-package-url/

Day Two Overview

The second day of the **CNA Fall Technical Workshop,** held on October 23, 2025, brought together CNAs to engage in surveys, feedback and reporting sessions, and informational presentations. The workshop was well attended, with 160 people attending and 95 CNAs represented. These sessions explored several key topics:

1. **CVE and VEX**: Alex Kreilein proposed adopting Common Security Advisory Framework (CSAF) and Vulnerability Exploitability eXchange (VEX) to improve how the CVE Program aligns to its mission and produces its desired outcomes: the reduced exploitation of systems and products, as well as improved patch velocity. Implementing VEX can improve standardization and programmability across CVE Records while taking a consumer-focused approach to capturing vulnerability data.
2. **ADP Pilot (Supplier ADP)**: Art Manion and Lisa Olson provided a breakdown of the upcoming SADP Pilot, which aims to explore the most practical methods of improving the newly established ADP Process through the context of suppliers. During the presentation, Art and Lisa provided the group with the scope, requirements, and implementation plan for the pilot, and discussed potential roadblocks.
3. **Community Feedback**: Katie Noble led a guided listening session to obtain a deeper understanding of the participant's opinions and evaluations of the current and aspiring state of the CVE Program. Overall, participants felt the CVE Program is doing a satisfactory job but noted concerns regarding data quality, transparency, and funding opportunities.
4. **CVE Reference Archive Pilot:** As the CVE Program was created 25 years ago, CVE Records have become outdated and/or broken. Kris Britton and Dave Welch introduced a pilot to the workshop that would spearhead the adjudication of these records, starting with a pilot. Through this work, information should be updated, preventing future issues and protecting information.
5. **5.2.0 Release of Record Format Roadmap:** Chris Coffin outlined the key updates for the Record Format Roadmap in the 5.2.0 version. These features included adding support for PURL, as well as providing a tightened-up schema, example records, and documentation. Not only has Version 5.2.0 been marked for release, but Chris also outlined the potential updates for the 6.0.0 version, including SSVC compatibility and the ability for more validation during ingest.
6. **Consumer Working Group:** Bob Lord and Jay Jacobs gave a presentation that outlined the responsibilities and goals of the Consumer Working Group (CWG), which is new. They described its purpose as being a mechanism for consumers to have a voice in the CVE Program. The Consumer Working Group has already collected user stories and is aiming to use them to create categories and bring people together to find critical solutions to complex problems.

Welcome & Keynote Remarks (Alicia Mink & Alex Kreilein)

Alicia Mink delivered a preview of the day's agenda and welcomed keynote speaker Alex Kreilein, Vice President of Product Security at Qualys. Alex delivered a presentation titled, "From Awareness to Action: Case for CSAF VEX."

1. **Distinguishing Outcomes vs. Output**: For the CVE Program to stay oriented to its mission, it should distinguish between its outcomes and output. Output includes the publication of CVEs and assignment of severity scores, which are functions of the program. The desired outcome, however, is the reduced exploitation of systems and products, as well as improved patch velocity. Maintaining this desired state, or outcome, as the Program's north star will help the Program become successful and deliver value to members of the CVE community.
2. **Tools and Approaches**: To achieve outcomes rather than outputs, new tools may need to be implemented across the Program such as VEX and CSAF. VEX and CSAF are machine-readable capabilities that allow standardization and programmability. VEX also provides assurance that a product is or is not affected by a CVE, supports automated triage with API support, RSS notifications, reduces mean time to remediate (MTTR) and mean time to close (MTTC), and builds trust between vendors, defenders, and regulators. Deploying VEX would position the Program as a user advocate.
3. **Applying VEX in CVE Records**: To deploy CSAF VEX and maximize its utility, Alex recommended using VEX in JSON or HTML to allow producers to publish machine-readable advisories, decreasing the inconsistency currently observed across CVE Records, and improving consumers' ability to assess risks. To demonstrate the use case, Alex encouraged participants to collaborate on interoperable standards such as OASIS, experiment with VEX and adopt machine-readable advisories, and test the tool for themselves. Nevertheless, participants flagged concerns with limitations, including that, with different ways to implement VEX and CSAF, achieving a standardized approach may not be straightforward.

Chat Links

- https://www.microsoft.com/en-us/msrc/blog/2025/10/toward-greater-transparency-machine-readable-vulnerability-exploitability-xchange-for-azure-linux
- https://github.com/zmanion/SBOM/blob/main/VEX_VDR.md
- https://github.com/SBOM-Community/documents?tab=readme-ov-file#vex
- https://github.com/anthonyharrison/lib4vex
- https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html#45-profile-5-vex
- https://github.com/openvex
- https://github.com/SBOM-Community/documents/blob/main/VEX/Reviewing_VEX_Practices/Reviewing_VEX_Practices.pdf
- https://dependencytrack.org/

- https://secvisogram.github.io/
- https://github.com/cisagov/CSAF

ADP Pilot (Supplier ADP) (Art Manion & Lisa Olson)

Art Manion, CVE Board member and co-chair of the Strategic Planning Working Group (SPWG), and Lisa Olson, CVE Board member and Principal Security Program Manager in the Microsoft Security Response Center, joined the Workshop to discuss the group's SADP Pilot. This pilot was created to examine the most efficient and effective methods for providing SADP information to consumers and suppliers. The SPWG is leading the efforts in defining and implementing the pilot. It is currently in the development stage but should be ready for deployment shortly.

1. **Authorized Data Publisher (ADP):** ADPs are authorized entities with specific scope and responsibility to enrich the content of CVE Records published by CNAs with additional, pertinent information (e.g., risk scores, references, vulnerability characteristics, translation).
2. **Supplier:** Suppliers are the entities that develop, maintain, or provide a Product. A supplier is typically responsible for and capable of investigating vulnerability reports and developing fixes or mitigations for vulnerabilities. "Supplier" is used broadly and includes common terms such as vendor, producer, maintainer, author, owner, manufacturer, and provider.
3. **ADP Pilot Purpose:** The ADP Pilot will consider changes to the schema and services to reduce dependency on software by examining how downstream software is potentially affected by a vulnerability in upstream software, and how a defender can obtain that information. The potential products being examined are from vendors including Microsoft, Oracle, Red Hat, HeroDevs, and Qualys.
    a. **Costs**: The ADP Pilot will examine how to mediate the costs that suppliers and users incur throughout the process of identifying vulnerabilities and communicating them to consumers.
    b. **Requirements**: To perform an accurate assessment, the pilot will require the identification of the upstream CVE IDs, downstream and upstream products, all nodes, owner of the SADP content, and the SADP authoritative for downstream products.
    c. **Implementation:** There will be two ways to test where the information in the SADP will live. The first will be to have SADP content use an SADP container within the CVE Record. The other method will be to have an SADP container refer to SADP content hosted by SADP (e.g., CVE Record, CSAF VEX Profile). Upstream CNAs will be notified of these additions to prevent any confusion. Feedback mechanisms will be put in place to ensure valuable comments are captured and considered when forming new guidance or rules.
    d. **Concerns:** A major consideration is that this pilot may cause an explosion of data that will be difficult to manage. To mediate this, the pilot creators will try to limit the scope and scale of the data collected. Additionally, CVE consumers may be misdirected to upstream CNAs and there may be competing information within SADPs that make it difficult to know the true source of the information.

Chat Links

- https://docs.google.com/presentation/d/12PHNIoEK9XdbIRUkk6D8ntbivUxprkMO4ccswNhRFbA/edit?slide=id.p1#slide=id.p1
- https://daniel.haxx.se/blog/2025/10/21/a-royal-gold-medal/
- https://youtu.be/6n2eDcRjSsk
- https://daniel.haxx.se/blog/2025/08/18/ai-slop-attacks-on-the-curl-project/

Guided Listening #2 (Katie Noble)

Katie Noble of the CVE Board joined the workshop to moderate and receive feedback on aspects surrounding CVEs through a guided listening session. To start the session, participants were asked to join a platform where they could vote on and write their opinions regarding various topics related to CVEs and cybersecurity. While many participants enjoyed the session, some found it duplicative of topics in the previous guided listening session.

1. **Number of CVEs Created a year:** Most respondents (26) said they create approximately 0-10 CVE Records a year. Another 11-50 and 101-500 CVE Records a year were the next most voted categories. The least-voted response was the creation of 500+ CVE Records a year.
2. **Most Used Tools:** The respondents voted that they were most likely to use Vulnogram as the main tool to create CVEs. Katie observed that these responses are statistically consistent with the results of previous surveys, noting that the lowest-rated platform was CVE Live.
3. **Feelings Toward CVE Program:** Regarding sentiment around the CVE Program, most respondents felt generally positive, rating it a 4/5. This showed confidence in the program, which was encouraging for all.
4. **Biggest Problem Facing CVE:** Data quality ranked the highest in reference to the largest problem facing the Program. Katie observed that the responses show the Program should prioritize giving risk-based decision-making information to consumers. Technical Modernization was also a major concern for the group. Funding concerns, balkanization, and transparency emerged as key concerns, as was observed in the results of the first day's listening session.
5. **Data Challenge**: Given that respondents ranked data as a major concern for participants, the question of how to define and fix the current data challenges increased engagement. Participants mentioned that the solution should begin with an overhaul of the CVE Record schema so that it is much harder to enter bad data. Additionally, respondents replied that more data does not equal better data, suggesting the CVE Program evolve to become the definitive source of truth for vulnerability information rather than relying on other entities for analysis.
6. **Data Consistency:** Respondents were asked about the type of information to establish as records' core principles and to make consistent for every CVE Record. The participants responded that CVE IDs are the most important, while CWE IDs provide less support in identifying vulnerabilities.
7. **Increased Support for CNAs**: When asked about how the CVE Program can better support CNAs, respondents said they would like to be given examples of what great reporting looks like versus just good reporting. They also requested that the Program share quality

audits/scores on published CVEs, make improvements to platforms such as Vulnogram, and increase global collaboration.

8. **Tool Recommendations and Best Practices**: Participants also emphasized the need for consistent and reliable funding streams to obtain tools that provide faster results. They also called for the consolidation of AI Tools as a possible first step.
9. **Future Priorities:** Participants had various ideas regarding the future of the CVE Program. They reiterated the importance of an updated framework, as well as the need for quality, modernization, and governance regarding data quality. Many also requested that the community be more involved in directing the priorities of the Program.

Chat Links

- Katie Noble: lady.noble.00@gmail.com

Reference Archive Experiment (Kris Britton & Dave Welch)

Kris Britton, Principal Software Assurance Engineer at MITRE and co-chair of the Automation Working Group (AWG), and Dave Welch, Chief Software Architect at HeroDevs, joined the workshop to outline its CVE Reference Archive Pilot. The pilot addressed various concerns regarding CVE Records that have become outdated or inaccessible over time. In response, the AWG has constructed an outline of a pilot that will sort and archive this type of CVE, resulting in more updated and accurate information for users.

1. **Reference Archive Pilot***:* The Reference Archive is being driven outside of MITRE's development and is part of a quality project. All information is open-source and anyone in the community can participate in the pilot.
    a. **Problem:** CVE Records have become broken or outdated, resulting in the loss of critical information tied to published CVE Records.
    b. **Solution:** The Reference Archive Experiment will protect information to prevent future issues by archiving content for all references in CVE Records into a repository, provide human/machine readable formats, and create a manner for the public to retrieve historical reference content based on CVE IDs.
    c. **Approach:** In the pilot, participants would use the API database to archive information. Additionally, users would store information in the S3 bucket through Amazon CloudFront.
    d. **Status:** The Reference Archive Experiment is still in the process of completing the first of two prototype stages. Stage 1 includes the initial demonstration of capability and Stage 2 will be beta testing. The beta testing will begin around January 2026. There is currently a demo that can be accessed through GitHub.

Chat Links:

- CVE Program Reference Archive Capability Requirements Document - Google Docs (Note: This document was approved by email votes via CVE AWG mailing list. Requirements were transcribed into GitHub issues in the CVEProject/cve-ref-archival repository.)

- https://www.flexera.com/products/security/software-vulnerability-research/secunia-research
    - Additional reference: https://secunia.com/advisories/42771 https://www.postman.com/herodevs/workspace/cve-archiver https://archive.cvearchiver.com/
- Dave Welch on CNA Slack: dave@herodevs.com

Record Format Roadmap – 5.2 and Major Release 6.0 Planning (Chris Coffin)

Chris Coffin, Lead Cybersecurity Engineer at MITRE, co-chair of the Quality Working Group (QWG), and CVE Board member, led a presentation on the current CVE Record Format schema and the QWG plans for future CVE Record Format updates. A brief overview of the CVE Record Format was also provided for those who are unfamiliar with the CVE Record Format schema.

1. **Introduction to the CVE Record Format:** The CVE Record Format is the blueprint for a rich set of JSON data that can be submitted by CNAs to describe a CVE Record. It determines the kinds of data required for CNA submissions and how the data can be provided/formatted. The most updated version is 5.1.1, which includes expanded support for CPE identifiers using the CPE Applicability language.
2. **CVE Record Format v5.2.0:** The soon-to-be-released CVE Record Format v5.2.0 will include support for Package URLs (PURLs), will disallow custom properties within the affected array and product items, and will include updates to several example CVE Records and improvements in documentation and infrastructure.
3. **CVE Record Format v6.0.0:** For the 6.0.0 version of the CVE Record Format, the QWG is planning to include official support for Stakeholder-Specific Vulnerability Categorization (SSVC), define additional data validations during ingest, and clean up other parts of the schema that are not actively used by CNAs.

Chat Links:

- Quick Start Guide for CPE Applicability Statements in the CVE Record Format
- https://github.com/package-url/purl-spec/
- https://github.com/CVEProject/cve-schema/blob/main/schema/docs/versions.md
- https://github.com/CVEProject/cve-schema

Consumer Working Group: Engaging the Community (Bob Lord & Jay Jacobs)

Bob Lord, a Senior Technical Advisor at the Cybersecurity and Infrastructure Security Agency (CISA), and Jay Jacobs, founder of Empirical Security, both co-chairs of the Consumer Working Group (CWG), outlined the origins and purpose of the new group and gave updates on its progress. These included the collection of user stories that will be utilized to inform the CWG on how it can best serve and represent consumers within the CVE realm.

1. **Consumer Working Group:** The CWG is a new working group that serves as a voice for consumers through identifying common patterns found throughout the current CVE lifecycle. Its main goal is to provide helpful feedback that fills knowledge gaps and brings innovation to the 25-year-old CVE Program.
2. **Current Status:** The CWG collected user stories from CNAs to identify various categories and create a community of people to help answer questions surrounding specific roles/tasks. The CWG aims to address problems within the current state of the CVE program and provide support for achieving desired outcomes.

Chat Links

- https://www.cve.org/ProgramOrganization/WorkingGroups#CVEConsumerWorkingGroupCWG
- https://docs.google.com/forms/d/e/1FAIpQLSeXbh-w0HAHID0Qsj47jEosqdTihJgahnkNEGf9cN14vKKmoA/viewform
https://docs.google.com/forms/d/e/1FAIpQLSeXbh-w0HAHID0Qsj47jEosqdTihJgahnkNEGf9cN14vKKmoA/viewform