User Experience Working Group

August 27, 2025

Participants

- Steve Christey
- Chris Coffin
- Matthew Coles
- John Keane
- Jon Moroney
- Przemyslaw (Rogue) Roguski
- Kathryn Stout

Agenda

- Introduction
- Weakness Remediation at Red Hat
- Open Discussion

Meeting Summary

- **Weakness Remediation**
  Przemek Roguski presented a new initiative at Red Hat that aims to leverage AI to analyze historical CVE data to map vulnerabilities.

Action Items

1. **Fortify Aviation:** Contact Alex Hoole about Fortify Aviation. (Chris Coffin)

Meeting Notes

Introduction (Chris Coffin)

- **Webinar:** John Keane reminded members about a webinar hosted by the National Academies of Sciences, Engineering, and Medicine. The webinar announced the findings of a new report that recommended steps for the Department of Defense to manage its software systems to mitigate and reduce cyber risk.
  - John Keane shared the webinar for the group's awareness.
  - The webinar can be viewed here: Defense Software for a Contested Future Report Release Webinar | National Academies.

Weakness Remediation (Przemek "Rogue" Roguski)

- **Background:** Przemek Roguski introduced a new initiative at Red Hat aimed at assisting product teams with weakness remediation. Przemek explained that Red Hat currently uses various weakness scanners during the build process to detect potential weaknesses in the source code of their products; however, Red Hat data show that 74% of weaknesses identified are false positives. He emphasized that the process is very time-consuming, especially when done in an automated way. Red Hat is examining the use of historical CVE

data and AI to map confirmed vulnerabilities to current weaknesses, providing prioritization suggestions based on past exploitations.

- **AI Mapping:** The AI mapping initiative involves using AI to analyze past vulnerabilities and their associated root causes to provide prioritization suggestions for current issues.
- **Matrix for Prioritization:** Przemek presented a matrix that lays out how to speed up the prioritization of weaknesses based on product type, such as operating systems and container-based products, and assigns impact levels like low, moderate, important, and critical to each category. The matrix will eventually be hardcoded into the prioritization pipeline.
    - **Example:** Przemek provided an example where memory buffer errors in an operating system are considered critical, whereas the same issue in a container-based product might be deemed low priority due to the nature of container environments.
- The matrix is based on Red Hat's internal information and manual assignment of weakness categories to product types. The next step would verify findings based on CVE data.
- Przemek described a two-phase prioritization process, starting with a fast initial assessment using the matrix and followed by a more detailed analysis using historical CVE data.
- **Use of CWE Data:** Steve Christey discussed the potential use of CWE data in the prioritization process, explaining the historical context of language-specific views in CWE and the challenges of maintaining them. Jon Moroney discussed the relevance of CWEs as informational components that feed into a broader system. Przemek noted that Red Hat is seeking examples of real-world use cases for CWEs.
- The group also discussed the role of different languages and tools in utilizing CWE data.
- **AI Tools:** John Keane recommended communicating with tool vendors to discuss the capabilities they have in preventing AI-based tools from using historical data to determine results are false positives. Chris shared that the CVE and CWE programs are conducting root cause mapping to deal with this issue. Steve shared that the CWE AI WG is examining approaches to cataloguing weaknesses, and the Root Cause Mapping WG is developing a chat bot to help users with root cause mapping. Matthew Coles raised concerns about AI tools potentially reproducing issues based on what is in their training sets or producing new ones, adding that OWASP and the Cloud Security Alliance are among the groups working to find solutions in this space.
- **Root Cause Mapping Accuracy:** Przemek noted that the accuracy of root cause detection and weakness assignment is not ubiquitous and depends on high level remote code execution in a relevant library. Steve shared that this issue has been appearing in work on the chat bot, noting that results are improved with more descriptive information or source code.
- **Red Hat Severity Rating:** Przemek also discussed work Red Hat is undertaking on CVSS, which will deliver additional information to the model he presented. Red Hat plans to start using CVSS scores in the future but currently uses its own severity ratings to provide more accurate risk assessments for their products.

- **AI Tools:** John Keane shared his experience with various AI and LLM tools, noting their potential for identifying issues and the importance of understanding the architecture of the code before making changes.

NEXT MEETING September 24, 2025