BlackBerry. Intelligent Security. Everywhere.

WHERE DO WE AIM?

THE STATE OF VULNERABLE SOFTWARE IDENTIFICATION AND ITS FUTURE

Apr 7, 2025

Andrew Suter

Senior Manager, BlackBerry PSIRT

Who am I?

- 18 years at BlackBerry
- 10 years in Product Security – PSIRT
- Participant in FIRST PSIRT and CVSS SIGs
- Previously participated in AutoISAC and ICASI

*Note: This presentation represents my own views and not necessarily that of BlackBerry Ltd, any FIRST SIGs or other groups I am apart of.

© 2025 BlackBerry. All Rights Reserved.

Agenda

- 2 main software identification schemes
- "Vulnrichment" initiatives
- Software producers as the authoritative source
- How Mitre and NIST can play a role

© 2025 BlackBerry. All Rights Reserved.

CPE and PURL

CPE

- Pros
  - Works well when you have a vendor and "product"
  - Dictionary available to enumerate known packages
  - Supports version ranges
- Cons
  - NIST/NVD is single point of failure for dictionary access and updates
  - Dictionary accuracy and maintenance is questionable
  - Poor for identifying varying distribution points

PURL

- Pros
  - Decentralized
  - Built with distribution points in mind
  - Good for libraries
- Cons
  - Low adoption
  - Generally assumes adoption of package repository (SWID and Generic available to mitigate)
  - Potential for PURL list to explode if all official and unofficial distribution points are included

    Ex. Curl would be available in rpm, deb, alpm, apk, etc

Both suffer from a lack of accurate data "in the wild"

Both are still useful!

© 2025 BlackBerry. All Rights Reserved.

"Vulnrichment" - NIST NVD

- Backlog continues to grow despite improvements [1]
- Program could become impacted by ongoing reductions
- Disputes regarding CVSS scoring have generated animosity
  - Curl project has been a vocal critic [2]
- Includes data from CISA ADP from CVE program, but not CNA provided data

From NIST.gov [3]:

We are currently processing incoming CVEs at roughly the rate we had sustained prior to the processing slowdown in spring and early summer of 2025. However, CVE submissions increased 32 percent in 2025, and that prior processing rate is no longer sufficient to keep up with incoming submissions. As a result, the backlog is still growing.

We anticipate that the rate of submissions will continue to increase in 2025. The fact that vulnerabilities are increasing means that the NVD is more important than ever in protecting our nation’s infrastructure. However, it also points to increasing challenges ahead.

[1] https://www.nist.gov/itl/nvd
[2] https://daniel.haxx.se/blog/2023/03/06/nvd-makes-up-vulnerability-severity-levels/
[3] https://www.nist.gov/itl/nvd#march1925

© 2025 BlackBerry. All Rights Reserved.

"Vulnrichment" - CISA

- Currently the only "Authorized Data Publishers" (ADP) for the CVE program
- Scope is limited
- As of Dec 10, 2024 CISA is no longer providing CPE data[1]
- Program could become impacted by ongoing reductions
- CISA defers to the CNA both before and after the CISA data is added
  - Won't override existing data
  - Will remove data if the CNA adds their own later

From CVE.org [2]:

For every new CVE Record, CISA ADP will publish the three relevant decision points in CISA’s SSVC triage process: Exploitation, Automatable, and Technical Impact. This is the first pass of enrichment which all new CVE Records will receive.

For those CVE Records that score at least one of:

- Technical Impact: Total
- Automatable: Yes
- Exploitation: Proof-Of-Concept, or
- Exploitation: Active

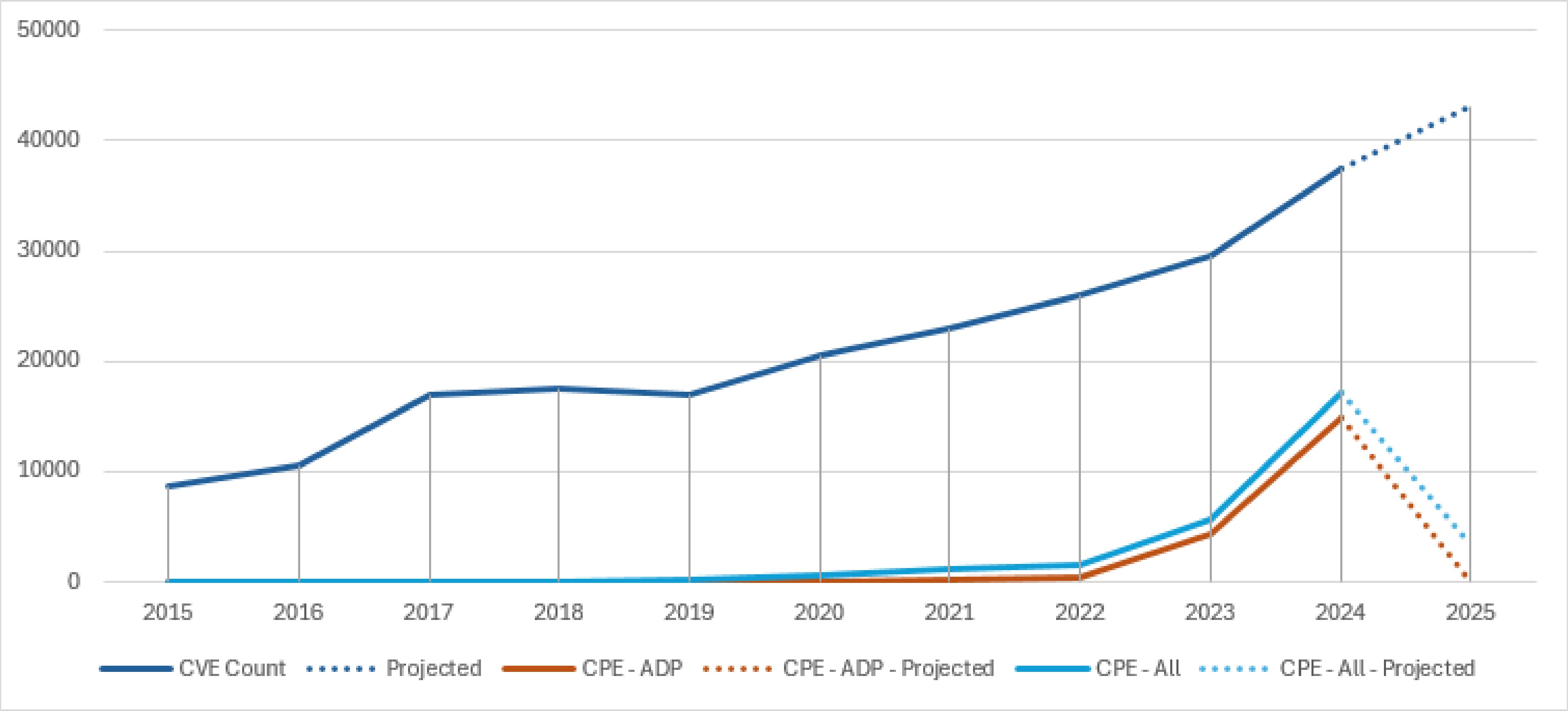
and are lacking one or more of CVSS, CWE, or CPE data, the CISA ADP will take a second pass of analysis to determine the missing CVSS, CWE, or CPE metric, and add those metrics to the CISA ADP container on those CVE Records.

[1] https://github.com/cisagov/vulnrichment?tab=readme-ov-file#cpe-strings
[2] https://www.cve.org/ProgramOrganization/ADPs

© 2025 BlackBerry. All Rights Reserved.

The Growing Problem

CVEs by year



© 2025 BlackBerry. All Rights Reserved.

How can we tackle the mountain?

Dividing up the work

- Software producers have unique insight into their software
  - Closed and open source maintainers generally have a greater understanding of the software than outsiders
- Software producers should be the authoritative source of impacted version ranges
- Software producers then have a responsibility to include the data whenever possible
  - This reduces the dependence on "vulnrichment" programs
- As we all tackle the growing challenge of managing security this data will help enable automation which is necessary to scale up

© 2025 BlackBerry. All Rights Reserved.

Where do Mitre, CISA and NVD fit in?

Filling in the cracks

- Mitre provides recognition to CNAs that provide enrichment data [1]
  - Expand this scope to include CPE/PURL data
  - Eventually these should be mandatory
  - "Affected" data is already mandatory but not necessarily CPE/PURL
- CISA and NVD can continue to fill in gaps for high priority CVE's that are missing pieces of data
  - Coordination is key to prevent duplication of effort
- NVD should delegate maintenance of the CPE dictionary, similar to Mitre's CNA program
  - Consider joining these programs together
  - NVD is adding thousands of CPE entries per month via email [2]

[1] https://www.cve.org/Media/News/item/blog/2025/03/25/CNA-Enrichment-Recognition-List-Update
[2] https://nvd.nist.gov/products/cpe/statistics

© 2025 BlackBerry. All Rights Reserved.

Final Thoughts

Calls to action – We're all in this together

- **NVD:**
  - Provide for delegation of CPE dictionary updates to producers (ie. CNAs)
  - Follow CISA's lead on vendor data being authoritative, if provided
  - Focus on enriching data for important vulns not covered by CISA
- **CISA:**
  - Focus on enriching data for vulns included in KEV and for rapid response
- **Mitre:**
  - Expand the scope of "vulnrichment" recognition to include CPE/PURL data
- **Software Producers:**
  - If we want to be seen as the authoritative source of information, we have an obligation to provide it

Mapping vulnerabilities to affected systems at scale is a complex problem, but the solution starts with quality machine readable inputs. With many hands this becomes light work.

© 2025 BlackBerry. All Rights Reserved.

Thank you

BlackBerry. Intelligent Security. Everywhere.

© 2025 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.