NIST's National Vulnerability Database Update and the Vulnerability Enrichment Ecosystem

VulnCon 2026

April 15, 2026

Harold Booth, Acting Group Manager, Software Security Group

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

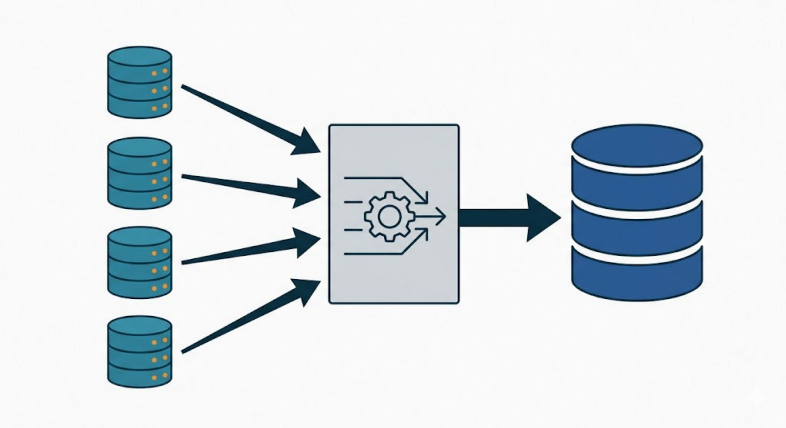
TLP: CLEAR

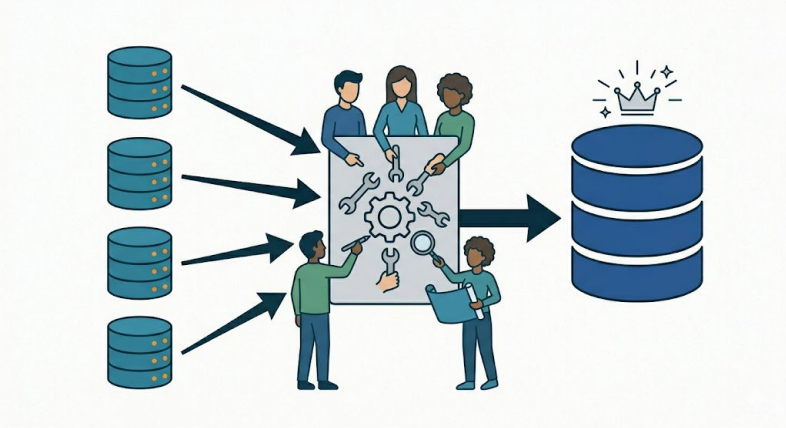
NVD – the 3,048 Meter View

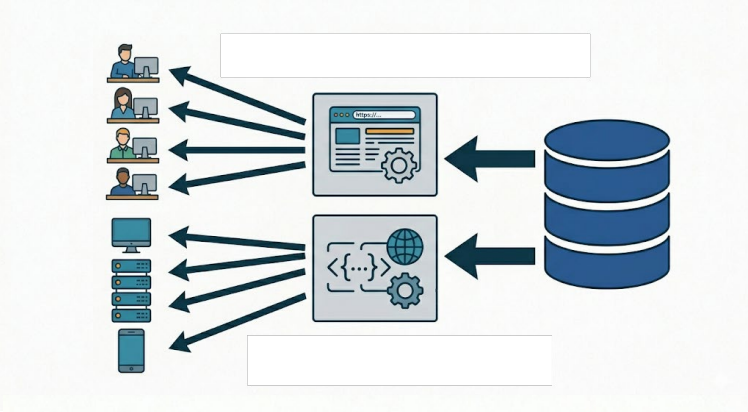
TLP: CLEAR

NVD Activities

The NVD serves multiple purposes for various groups within the vulnerability management ecosystem:







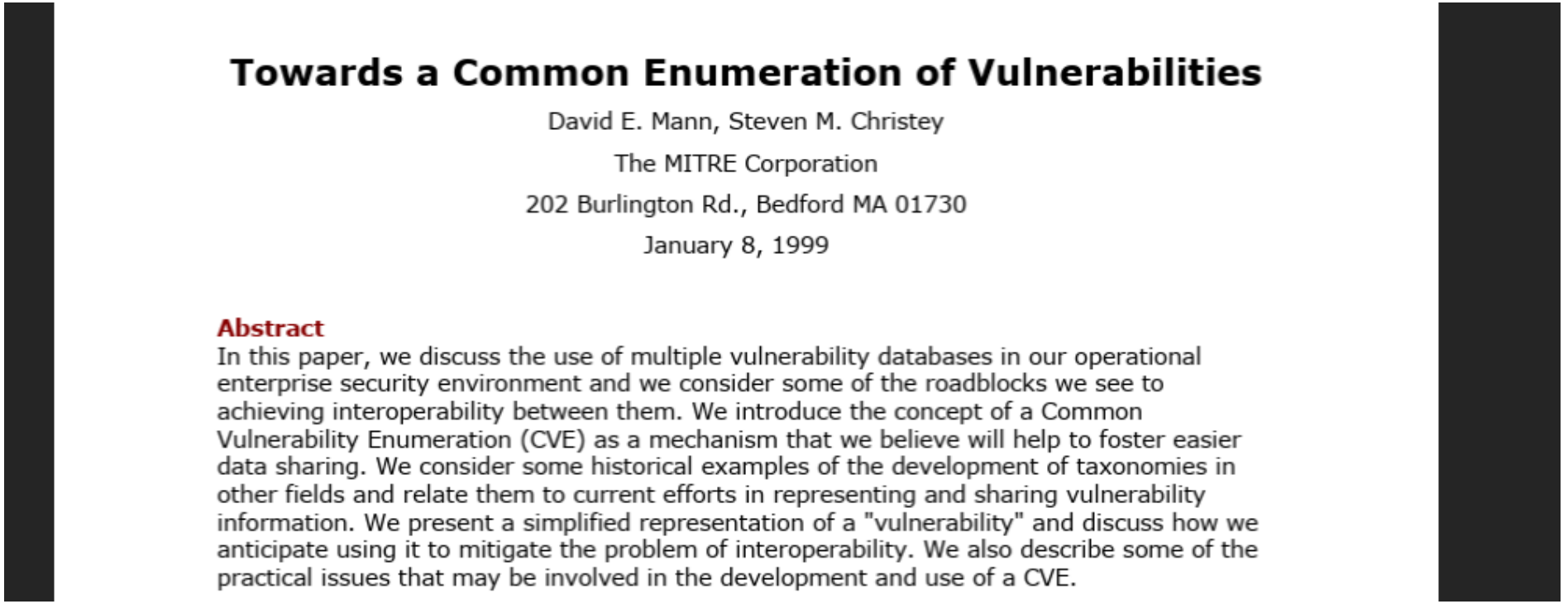
Images: Generated by Google's Gemini 3 (Fast) April 12, 2026

Some History

Image: Generated by Google's Gemini 3 (Thinking) April 14, 2026

Early CVE Identifier

- **Identity Interoperability**
- **Description**
- **Reference Links**



Towards a Common Enumeration of Vulnerabilities

David E. Mann, Steven M. Christey

The MITRE Corporation

202 Burlington Rd., Bedford MA 01730

January 8, 1999

Abstract

In this paper, we discuss the use of multiple vulnerability databases in our operational enterprise security environment and we consider some of the roadblocks we see to achieving interoperability between them. We introduce the concept of a Common Vulnerability Enumeration (CVE) as a mechanism that we believe will help to foster easier data sharing. We consider some historical examples of the development of taxonomies in other fields and relate them to current efforts in representing and sharing vulnerability information. We present a simplified representation of a "vulnerability" and discuss how we anticipate using it to mitigate the problem of interoperability. We also describe some of the practical issues that may be involved in the development and use of a CVE.

National Vulnerability Database

- **Integrated with CVE**
- **Provided additional Metadata**
  - Product
    - Vendor, Product, Version->CPE
  - Categorization
    - CWE
  - CVSS 1.0 -> 3.1
  - Reference Tagging

Industrialization of CVE

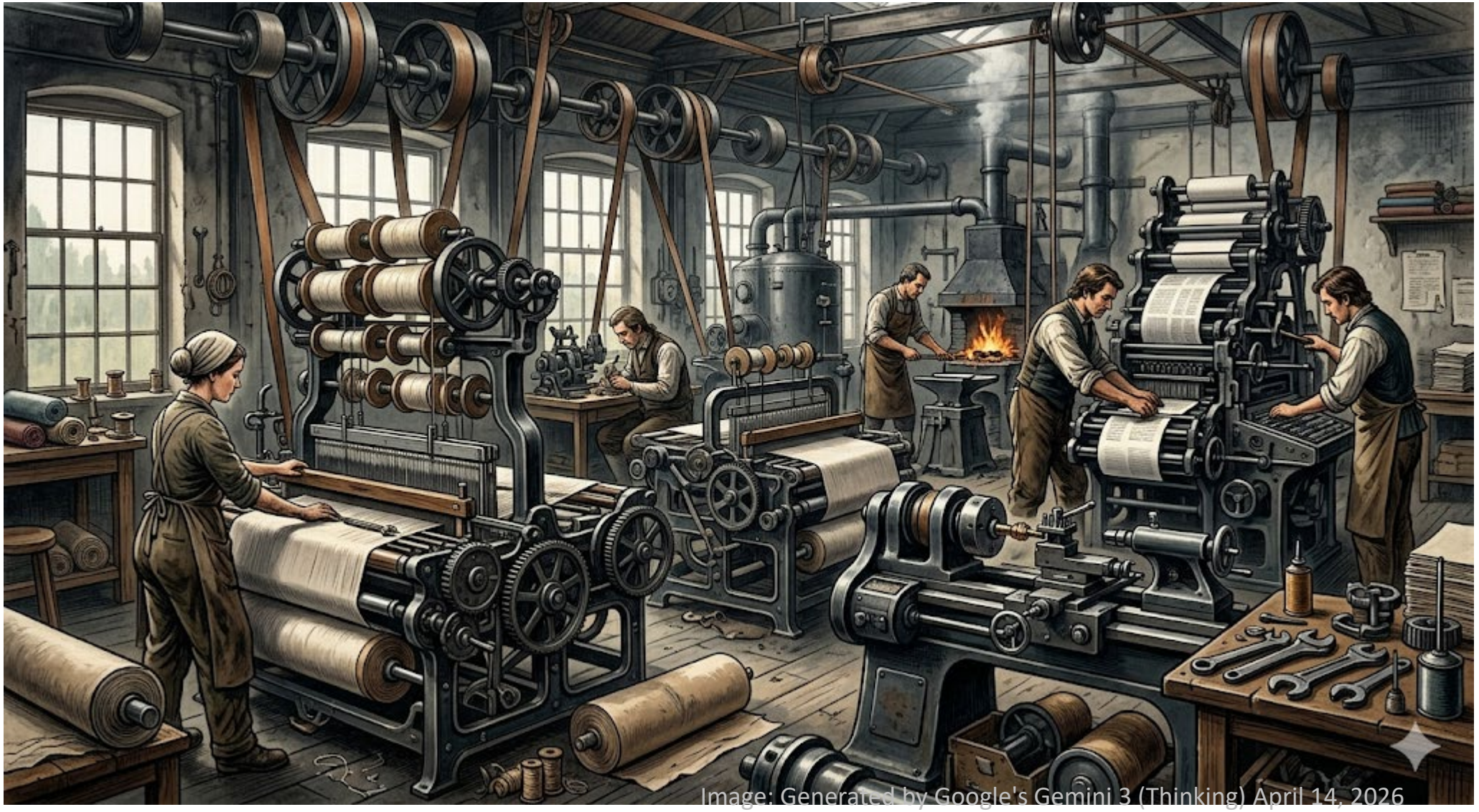


Image: Generated by Google's Gemini 3 (Thinking) April 14, 2026

Federating CVE Publication

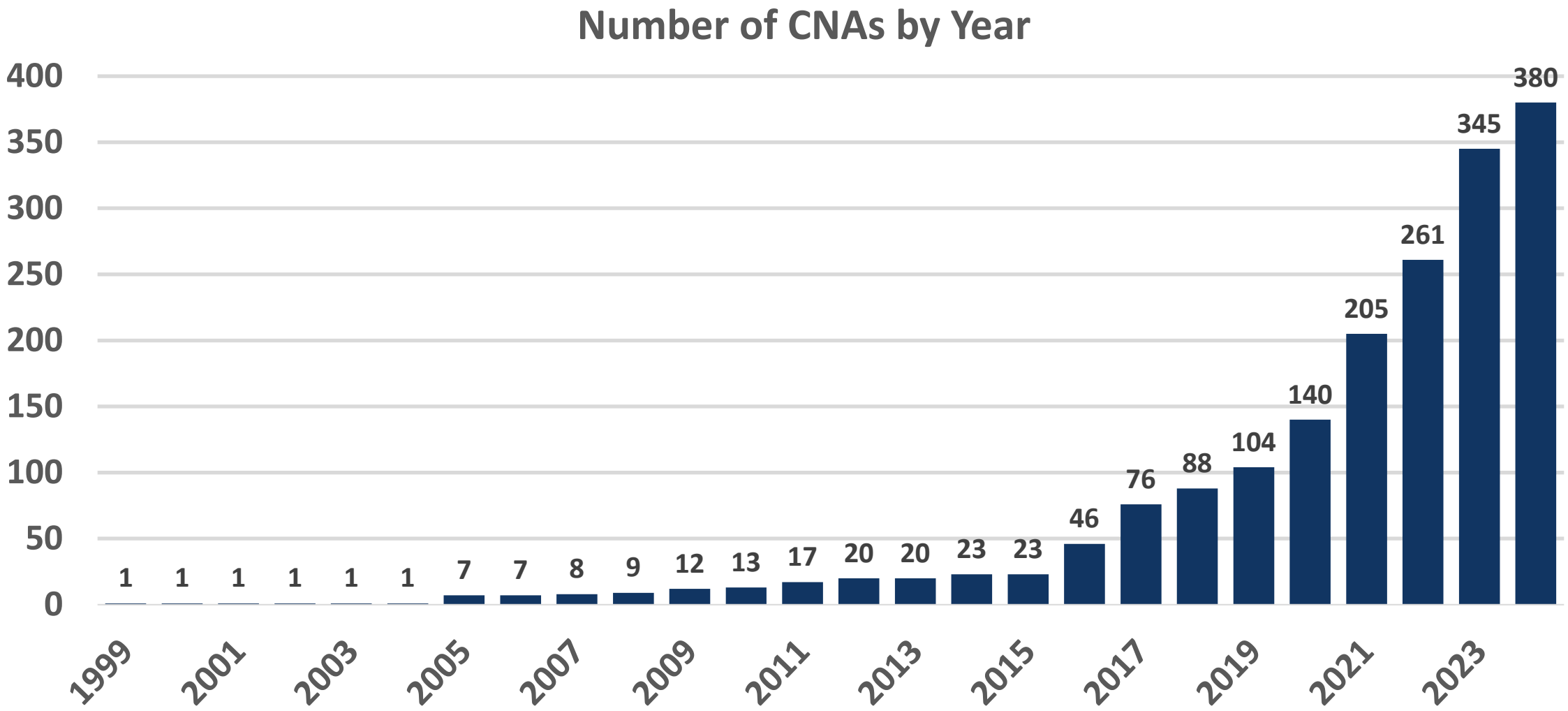
- Began about ~2016
- Increased Role for CNAs
- Independently Publish CVE IDs

Data Quality Questions

- Abstraction
- Counting
- Incomplete or Insufficient Descriptions

CNAs

April 2026: 502 – source: cve.mitre.org



We want this

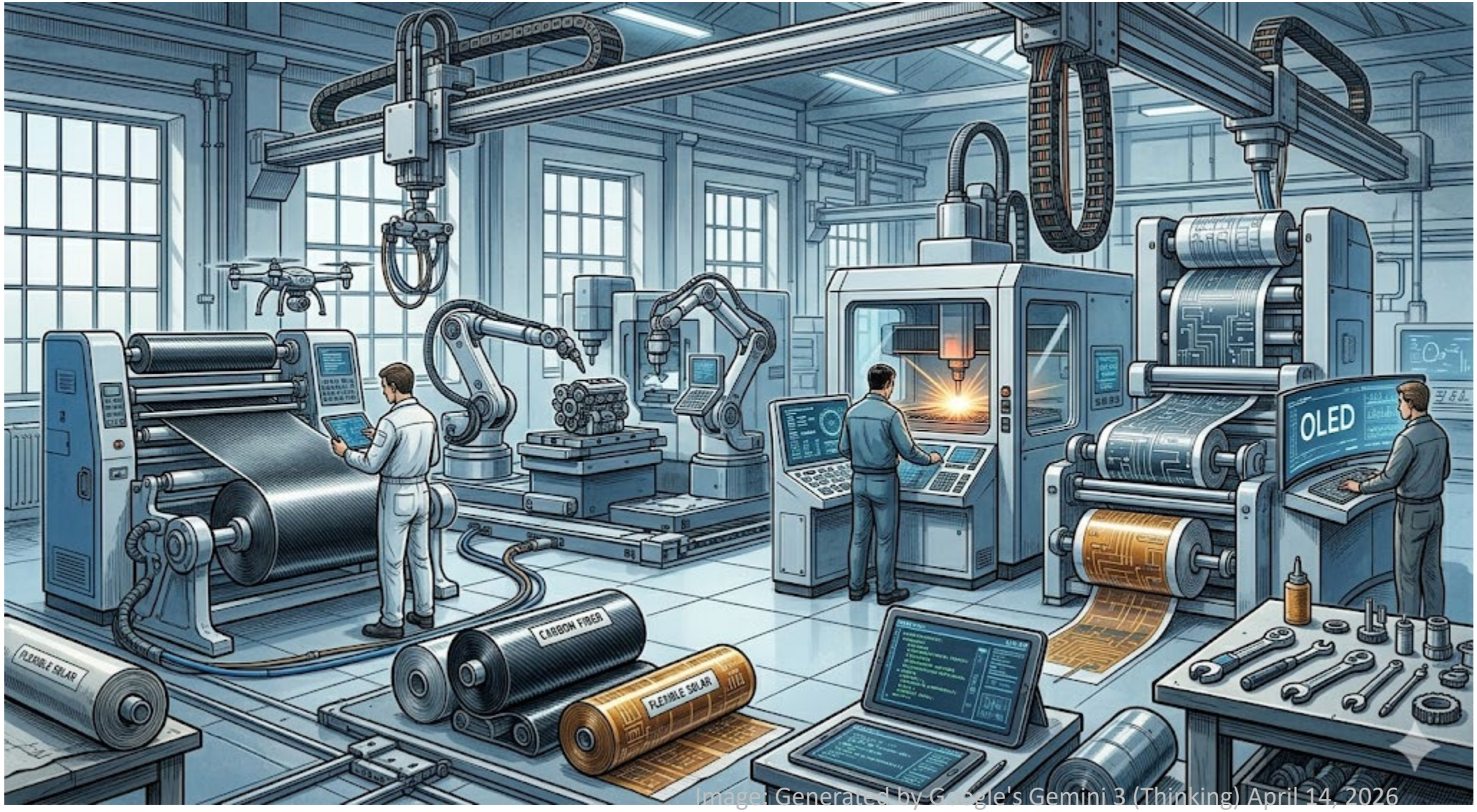


Image Generated by Google's Gemini 3 (Thinking) April 14, 2026

But we have some of this going on

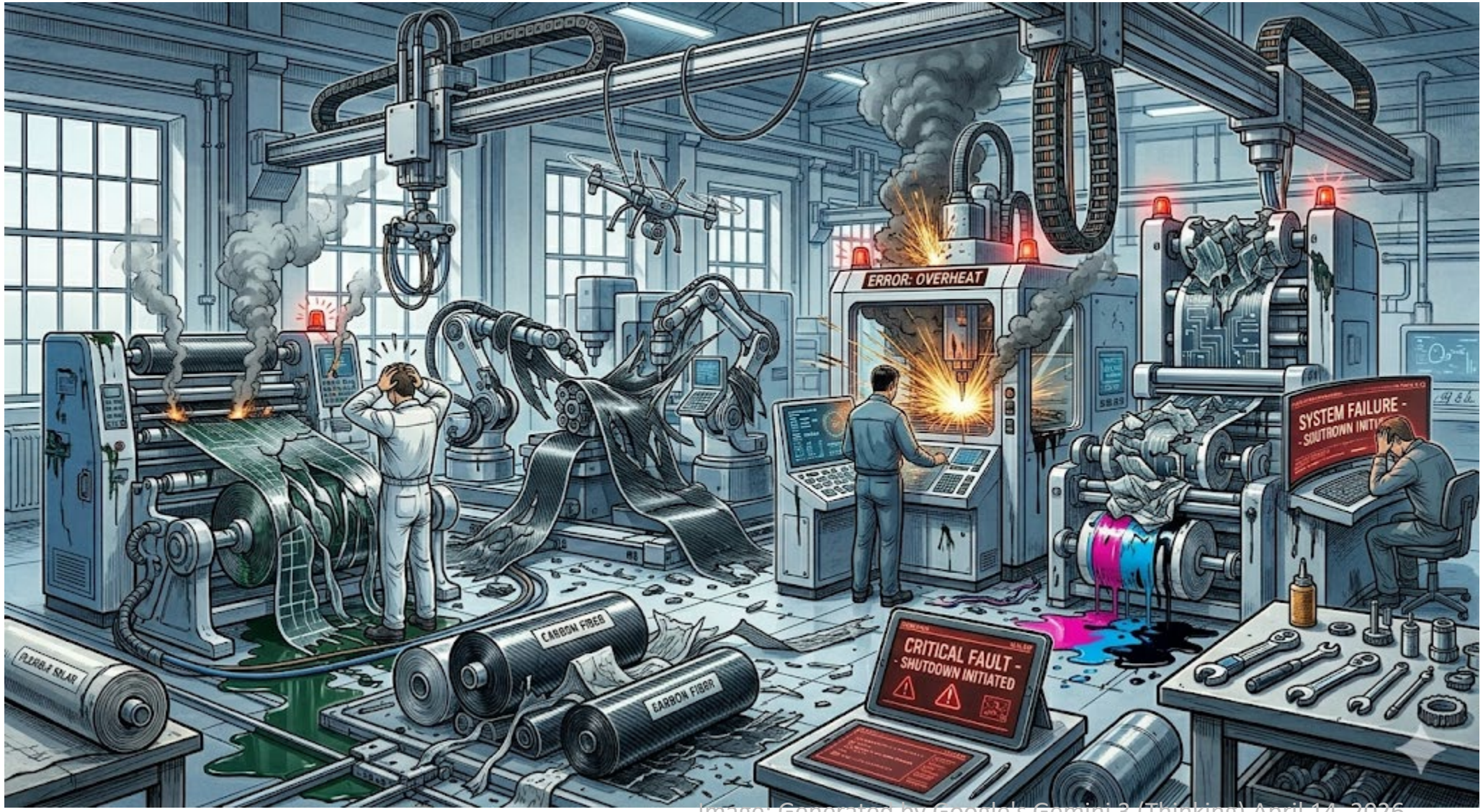
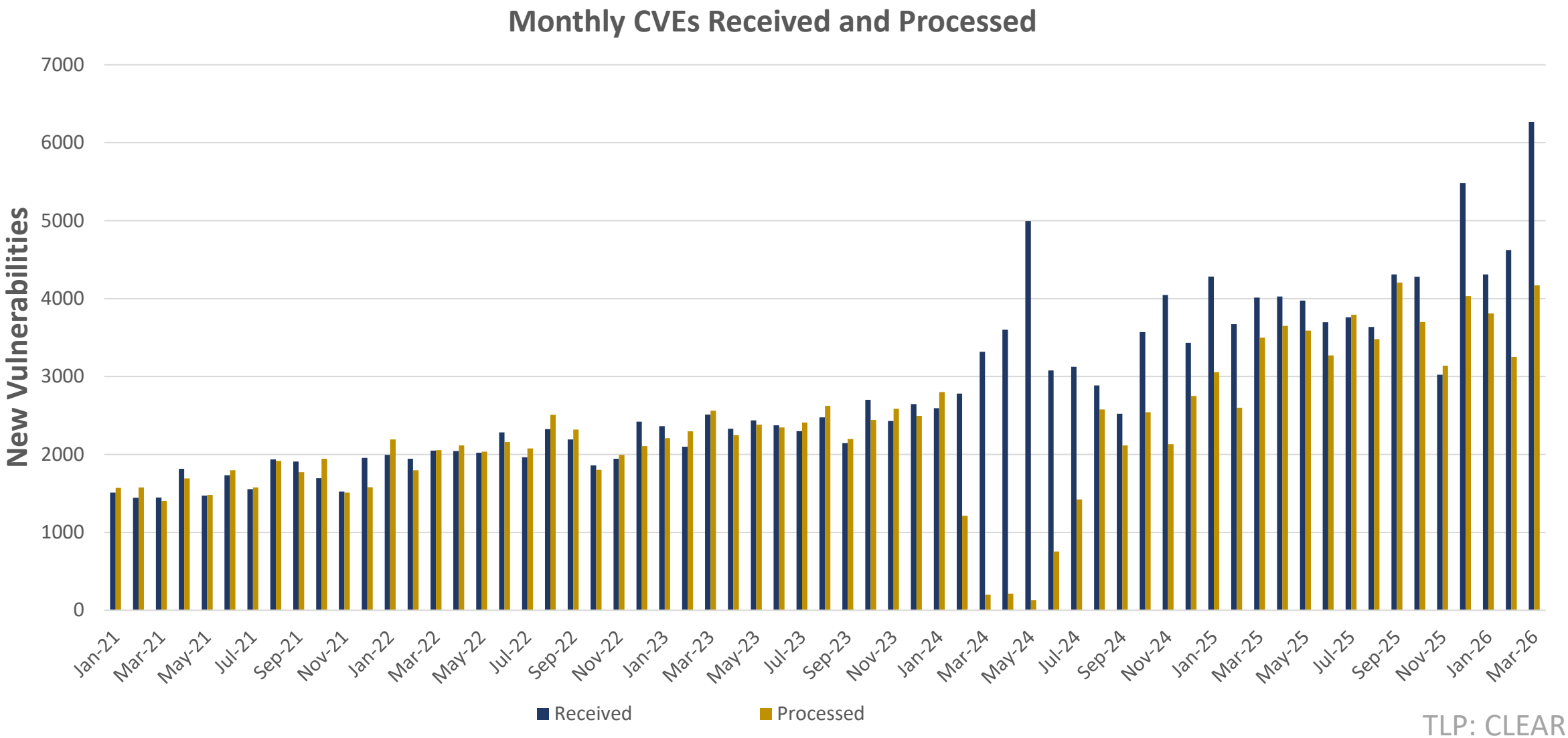


Image: Generated by Google's Gemini 3 (Thinking) April 14, 2026

CVE Production Trends



TLP: CLEAR

CVE Data Quality

Still exist

- Abstraction
- Counting
- Incomplete or Insufficient Descriptions
- Stable References

New Questions

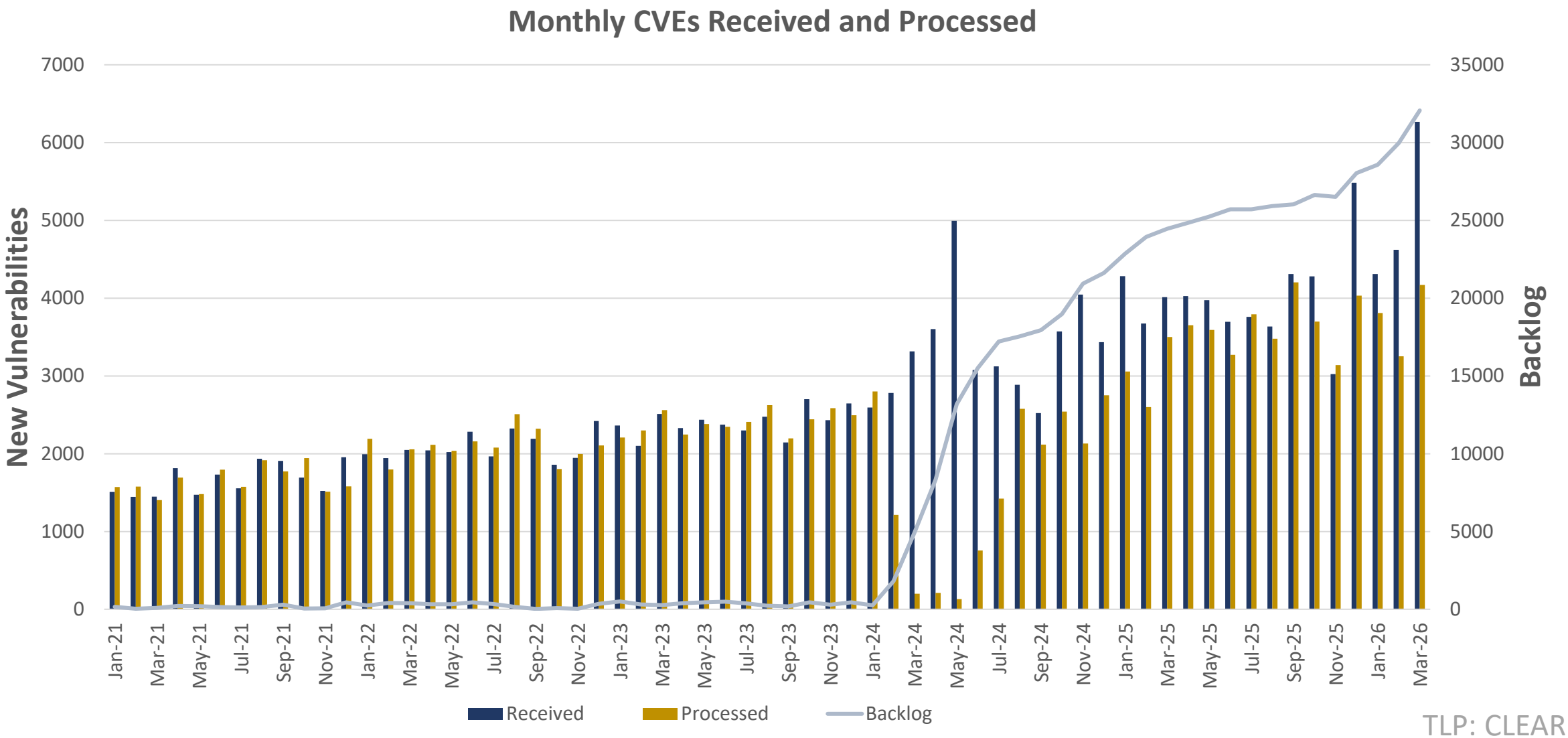
- Affected
- Consistent Scoring
- No Scores

Quality for What Purpose?

High-Quality Vulnerability Information

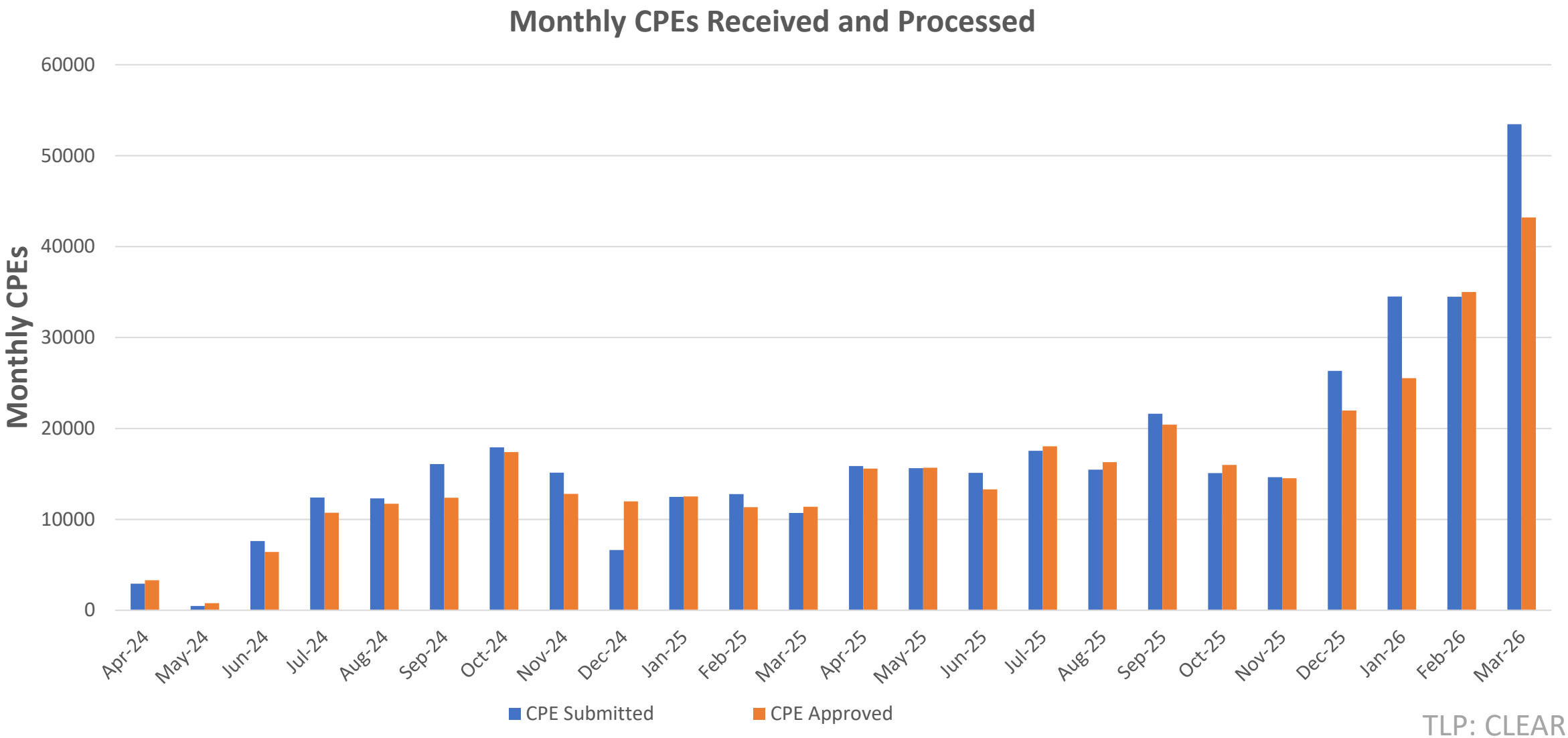
- Who benefits?
- What is most valuable?
- Who has best access?
- How is it shared?

CVE Production Trends



TLP: CLEAR

CPE Production Trends (2-Years)



NVD Short-term Changes

- New Prioritization Criteria
- Streamlining Severity Scoring
- Handling of Modified CVEs
- CVE Backlog
- New Status Labels

Prioritization Criteria

- CVEs appearing in CISA's Known Exploited Vulnerabilities (KEV) Catalog.
  - Within one business day of addition to the KEV Catalog
- CVEs for software used within the federal government
- CVEs for Critical Software as defined by Executive Order 14028

EO Order 14028 Critical software is defined as any software that has direct software dependencies (and one or more components with at least one of these attributes):

- It is designed to run with elevated privilege or managed privileges
- It has direct or privileged access to networking or computing resources
- It is designed to control access to data or operational technology
- It performs a critical function to trust, or it operates outside of normal trust boundaries with privileged access

NVD Short-term Changes

- New Prioritization Criteria
- Streamlining Severity Scoring
- Handling of Modified CVEs
- CVE Backlog
- New Status Labels

NVD Looking Ahead

- Automation
  - LLMs and AI-Agents
  - “Old-Fashioned” RPA
- Federation
  - CNAs
- Crowd-Sourcing
  - APIs and Web Interface

What Data?

Product Information

Priority

Impact

Remediations

Other?

Product Information

- Identifier
  - Unique Instance of a Product
- Applicability (or Affected) Use Case
  - Sets or Grouping of Products
  - Before, After, <, >
- Management and Sharing

Other Metadata

- Priority and Impact
  - CVSS
  - VulntologY
  - SSVC
- Remediations
  - Patches
  - Mitigations
- Other?

How Can You Help?

Reach out to me or email nvd@nist.gov

Participate in workshops and events

- Upcoming CPE Workshop for Hardware planned – look for announcements

Participate in open projects

Questions?