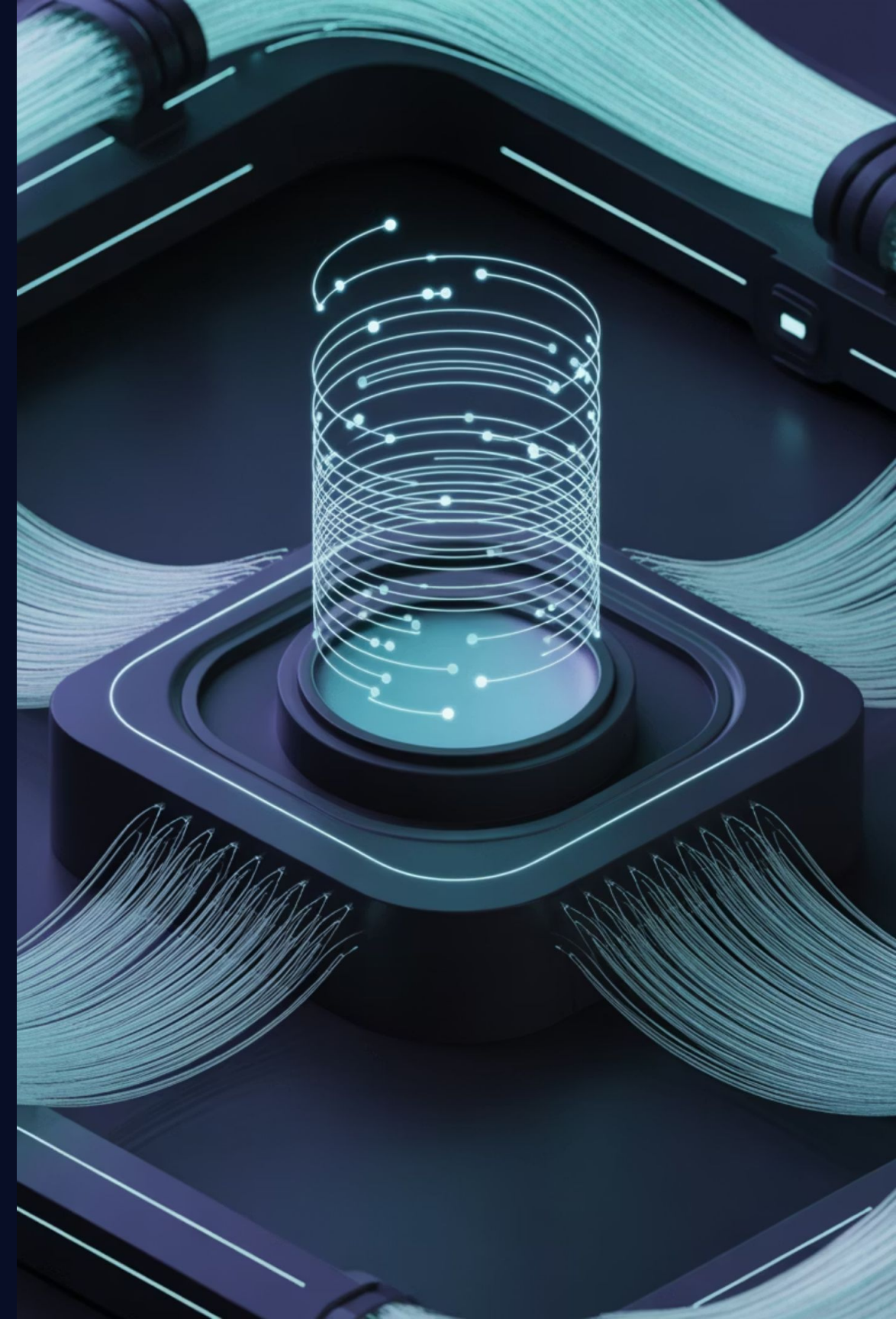


# The CVE Crisis: Navigating the Post-NVD Monolith Era

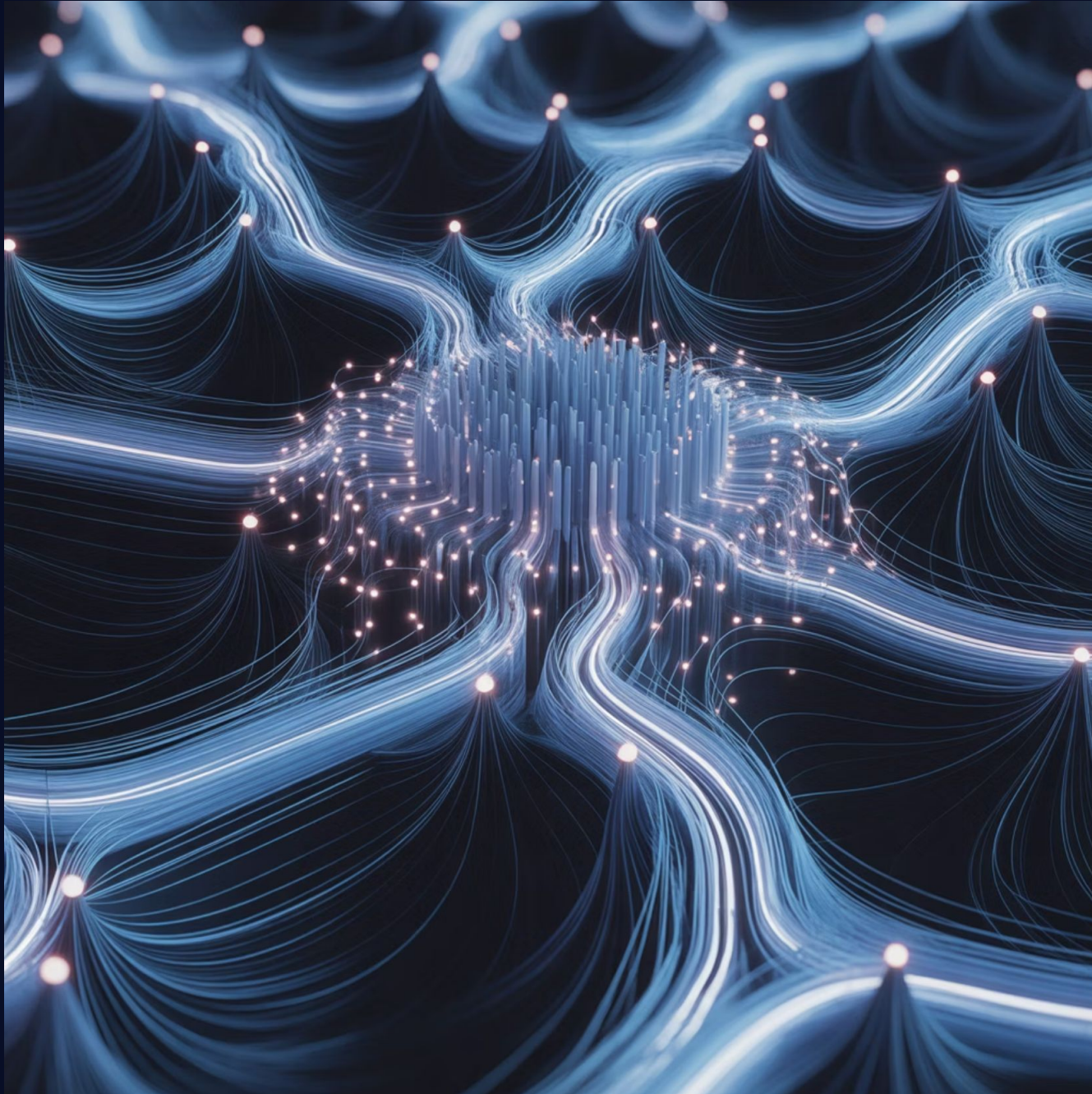
Strategies for AppSec Professionals in a Fragmented Landscape

Jerry Gamblin, Founder, RogoLabs.net





# About Me: Jerry Gamblin



## ***Researcher. Builder. Hacker. Traveler.***

- Founder of RogoLabs.net
- Started in government (security & cryptography)
- Regular speaker (DEF CON, BSides, 44CON)
- Member of EPSS SIG and CVE working groups
- Passionate about data-driven security.

# RogoLabs: Open-Source Initiative

Bringing clarity to vulnerability intelligence through open-source tools



[cve.icu](https://cve.icu)

Open-source intelligence platform for CVE analytics and trend visualization



[cveforecast.org](https://cveforecast.org)

A simple tool to forecast the growth of CVEs over time



[patchthis.app](https://patchthis.app)

A project to simplify and streamline the patching process



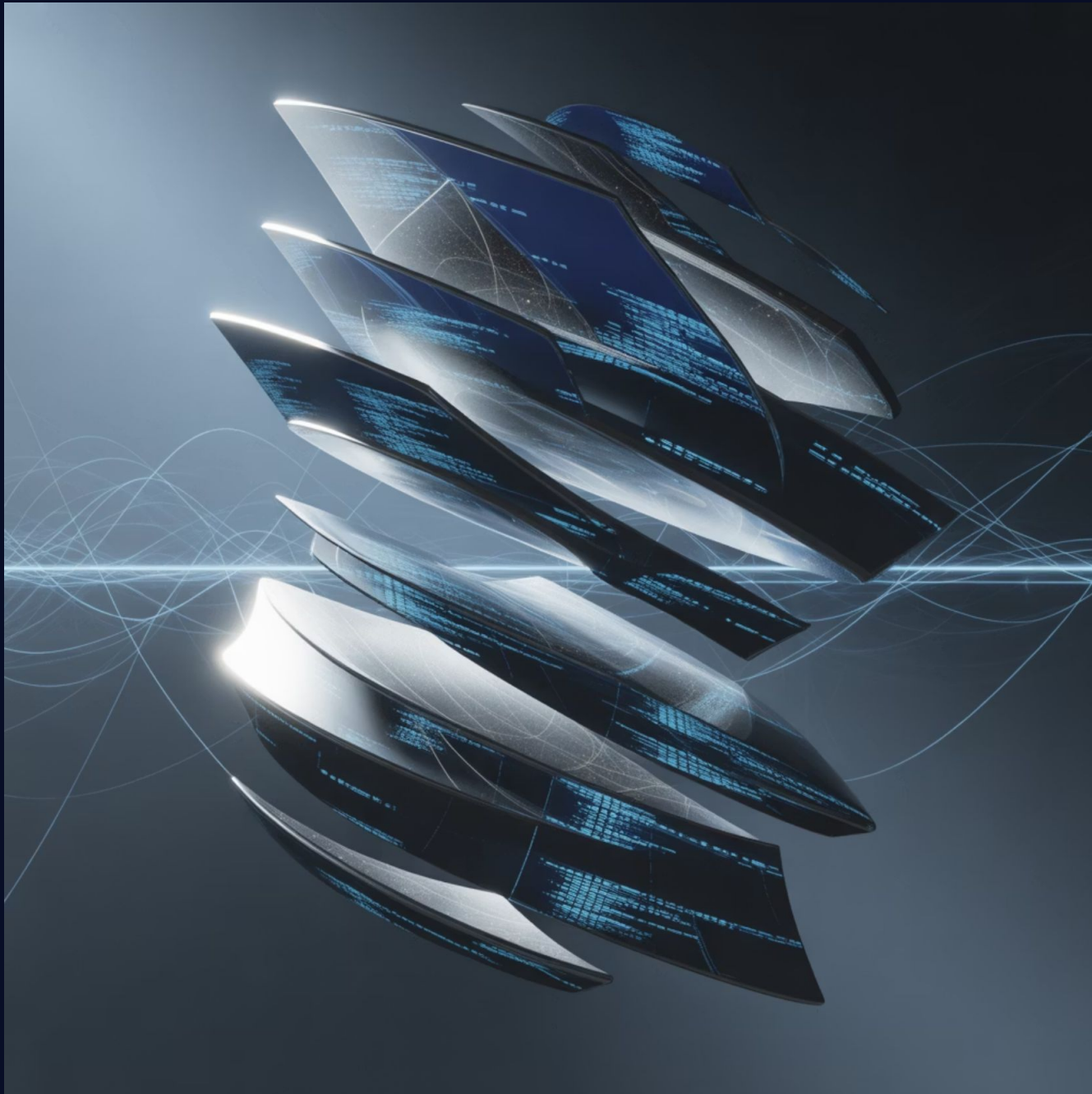
[CNAScoreCard.org](https://CNAScoreCard.org)

New project evaluating performance and data quality of CVE Numbering Authorities

Philosophy: I don't just talk about problems; I build open source solutions.



# The Problem in a Nutshell



## What is the NVD?

The U.S. National Vulnerability Database – the world's canonical source for *enriched* vulnerability data.

## What is Enrichment?

Adding critical metadata like affected products (CPE), vulnerability type (CWE), and severity score (CVSS).

## The Crisis:

Since early 2024, the NVD has failed to keep up with enriching new CVEs, creating a massive backlog.

## The Impact:

Automated security tools are breaking, patch prioritization is failing, and organizational risk is increasing systemically.



# The Crisis by the Numbers (Mid-2025)

25,000

Unenriched CVEs

Vulnerabilities currently awaiting  
analysis in backlog

131

Daily CVE Submissions

New vulnerabilities added daily

111

Daily Analysis Rate

Maximum NVD processing  
capacity

45%

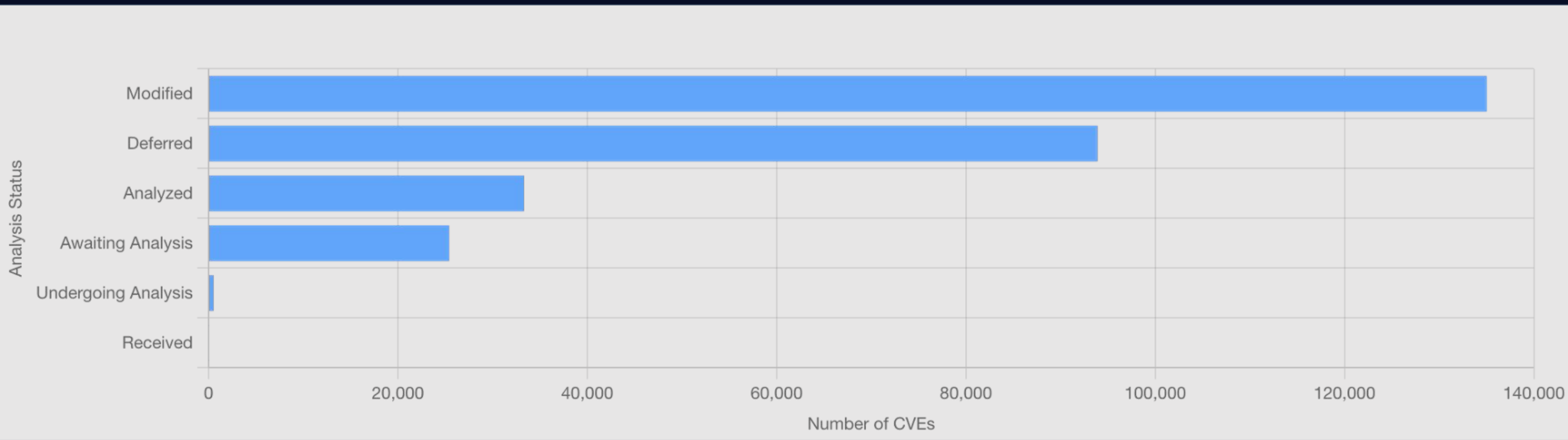
Exploited But Unanalyzed

Vulnerabilities on CISA's "Known  
Exploited" list without NVD  
analysis

The backlog is projected to exceed **30,000** vulnerabilities by the end of 2025.

NVD has begun re-categorizing vulnerabilities from 'Awaiting Analysis' to 'Undergoing Analysis.'

This re-categorization makes it difficult to track the actual backlog size. All numbers in this section are sourced from [cve.icu](https://cve.icu).





# Institutional Power Shift: NIST vs. CISA

1

## NIST's Position (NVD Operator)

- Overwhelmed by a 32% YoY increase in vulnerabilities
- Resource constraints limiting response capabilities
- Hired contractor (Analygence) to help process backlog
- Exploring AI solutions for faster analysis
- Now under formal OIG audit (May 2025)

2

## CISA's Position

- Decisively stepped in to fill the vacuum
- Now the new center of gravity for operational vulnerability management

### Known Exploited Vulnerabilities (KEV) Catalog

The *de facto* priority list

### "Vulnrichment" Program:

CISA now enriching CVEs itself and publishing data on GitHub with a focus on SSVC.



# Case Study: The SharePoint "ToolShell" Exploit (July 2025)

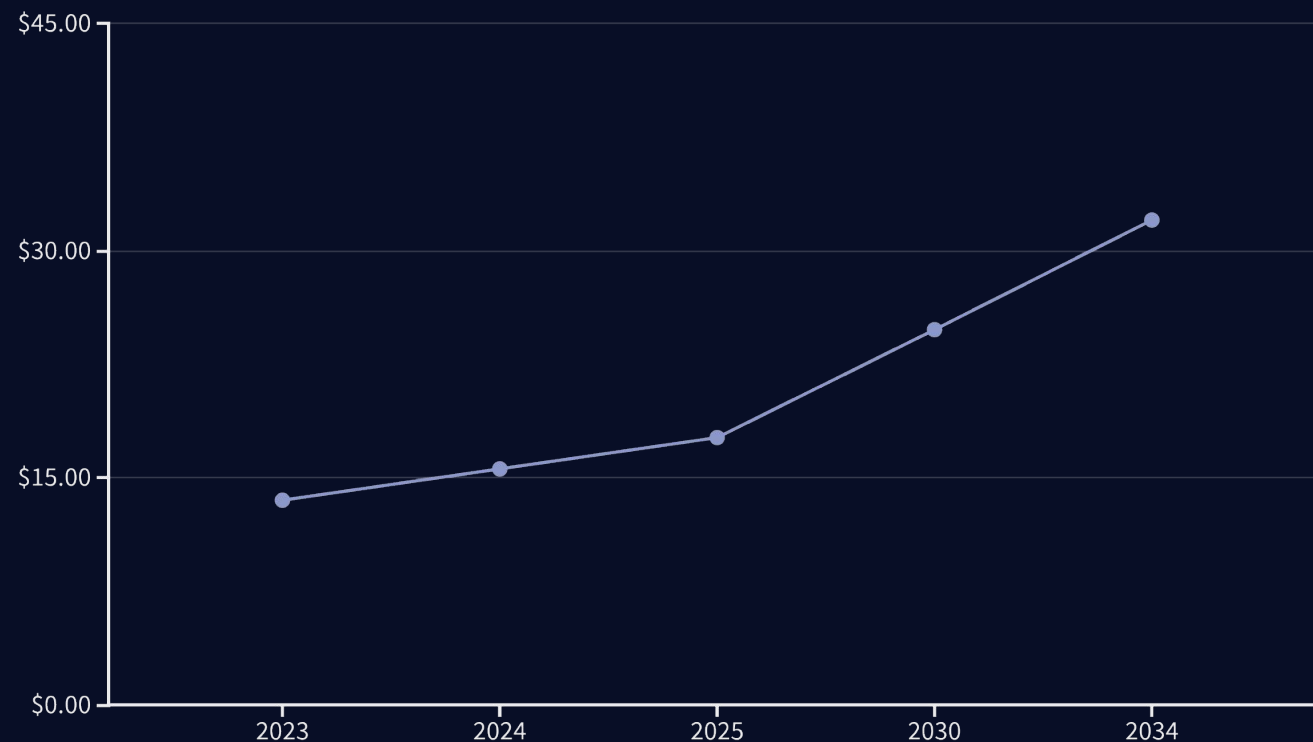


**Key Takeaway:** This shows the new dynamic in action. CISA is now the rapid response authority. The ecosystem has "unbundled"—the NVD is no longer the single source of truth.





# The Commercial Response: Monetizing the Intelligence Gap



Vulnerability Management Market Growth

## Key Commercial Players

- Flashpoint (VulnDB): 100,000+ vulnerabilities
- Vulners: Real-time intelligence platform
- Vulncheck: Vulnerability visibility platform

## Value Proposition

**Speed:** Intelligence faster than NVD

**Coverage:** Include non-CVE vulnerabilities

**Context:** Proprietary scores and exploit predictions

The Downside: Creates a divide between enterprises who can afford premium feeds and SMEs/non-profits who cannot



# The Open Source Counter-Movement

**A Different Philosophy:** Building a decentralized, transparent, and community-driven alternative to commercial vulnerability intelligence

## [OSV.dev](https://osv.dev) (Open Source Vulnerabilities)

A **federated aggregator**, not a monolithic database

- Pulls data from GitHub, Python's PyPA, RustSec, Linux distros, and more
- Massive adoption: handling over 900 queries per second at peak

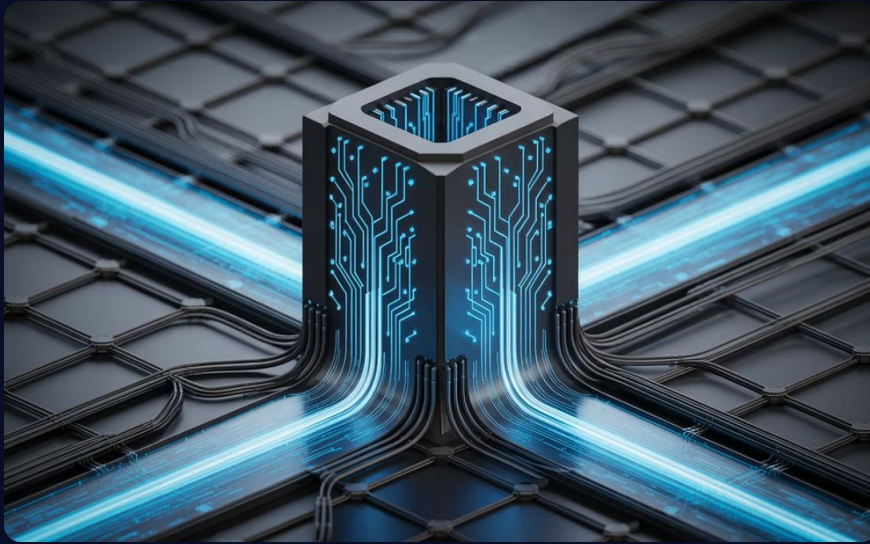
## Community-Driven Tools

Projects like [cve.icu](https://cve.icu) and [cveforecast.org](https://cveforecast.org) fill analytical gaps

- Democratizing access to vulnerability intelligence
- Creating transparency where official sources have failed

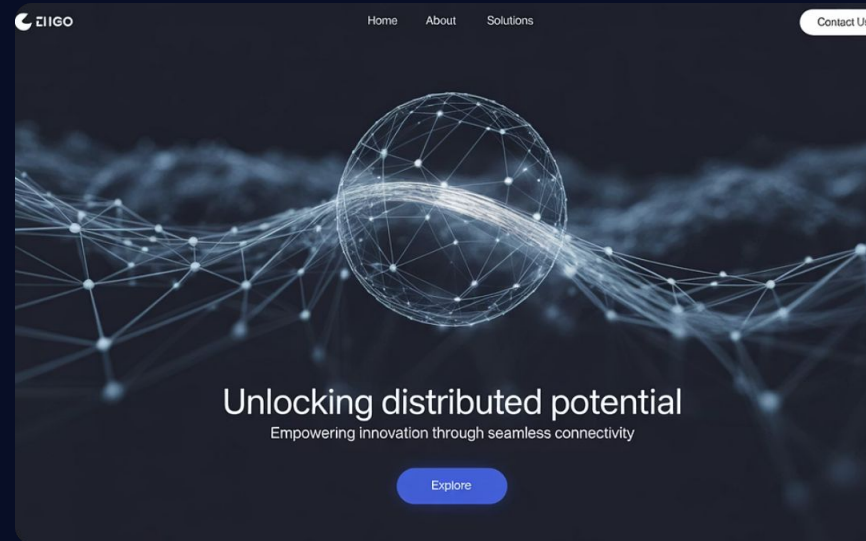


# The New Architecture: Federated vs. Centralized



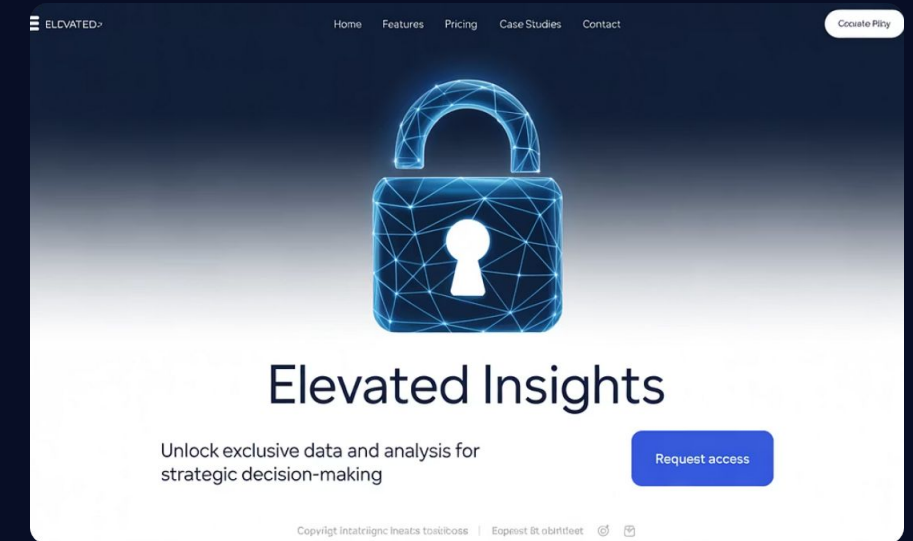
## Centralized Model (Old NVD)

- Single, monolithic database
- Single point of failure
- Bottlenecked processing
- Rigid schema requirements



## Federated Model (OSV.dev)

- Distributed network of databases
- Resilient to individual failures
- Scalable processing capacity
- Flexible data formats



## Commercial Aggregator

- Centralized but proprietary
- Curated, high-confidence data
- Premium intelligence services
- Additional contextual analysis

# The Regulatory Driver: EU's



## Landmark EU Regulation

Makes manufacturers legally responsible for the security of their products throughout the entire lifecycle

## Key Mandate

Manufacturers must notify the EU's cybersecurity agency (ENISA) of any actively exploited vulnerabilities **within 24 hours**

## The Impact

Will create a massive, decentralized flood of new vulnerability disclosures, making a federated model like [OSV.dev](https://osv.dev) essential for the future

Companies unable to track and respond to vulnerabilities face penalties up to €15 million or 2.5% of global revenue



# The AI Double-Edged Sword



## AI for Attackers

According to recent industry reports, **an estimated 40% of all cyberattacks are now AI-driven**

- Hyper-realistic phishing campaigns that bypass traditional filters
- Adaptive malware that evades signature-based detection
- Automated vulnerability discovery in previously unexamined code
- Sophisticated lateral movement using behavioral mimicry



## AI for Defenders (A Necessity)

No longer optional – defenders must leverage AI to keep pace

- Improves threat prioritization.
- Increases SOC efficiency with accelerates analysis
- Enables predictive defense through pattern recognition

**The New Arms Race:** It's no longer just about exploits; it's about who has the most intelligent prioritization AI



# A Modern Framework: Risk-Based Vulnerability Management


**The Goal:** Move beyond just patching every CVE. Focus limited resources on managing *actual risk*.



## Discover

You can't protect what you don't know.

- Maintain comprehensive asset inventory
- Hardware, software, cloud resources
- Code dependencies and supply chain
- Continuous discovery, not point-in-time



## Prioritize (The Core)

Replace simple CVSS scores with multi-factor model:

- Is it being exploited? (Check CISA KEV, EPSS score)
- How critical is the asset? (Mission-critical? Internet-facing?)
- What is the environment? (Mitigating controls like WAF?)



# RBVM Framework (Continued)



## Remediate

Integrate security into operations.

- Automate ticket creation in ITSM systems
- Embed security scanning (SAST/SCA) into CI/CD
- Shift left: catch vulnerabilities in development
- Track remediation SLAs based on risk tier



## Communicate

Translate technical data into business risk.

- Track MTTR for critical flaws
- Measure overall risk reduction over time
- Identify "vulnerability chaining" where multiple low-severity flaws create critical attack paths

⚠ Organizations focused solely on CVSS scores are **6.8x more likely** to experience a major security incident compared to those using a risk-based approach.

# Conclusion & Key Takeaways



- 1 The NVD-centric world is over. I've found the ecosystem is now fragmented and federated.
- 2 I advise you to adapt or fall behind. Passive consumption of a single data feed is a losing strategy.
- 3 I recommend becoming a sophisticated integrator. Build your intelligence stack from multiple sources: CISA KEV, commercial feeds, and open-source projects.
- 4 I urge you to prioritize ruthlessly. Move from a CVSS-only mindset to a true Risk-Based model that layers exploitability, business context, and environmental factors.
- 5 I believe embracing AI and automation is crucial. These are no longer luxuries; they are core necessities for survival in the modern threat landscape.



# Questions?

Thank you for your time. I'm happy to answer any questions you may have.



**Email**

[jgamblin@rogolabs.net](mailto:jgamblin@rogolabs.net)



**LinkedIn**

[linkedin.com/in/jerrygamblin](https://www.linkedin.com/in/jerrygamblin)



**Website**

[rogolabs.net](http://rogolabs.net)