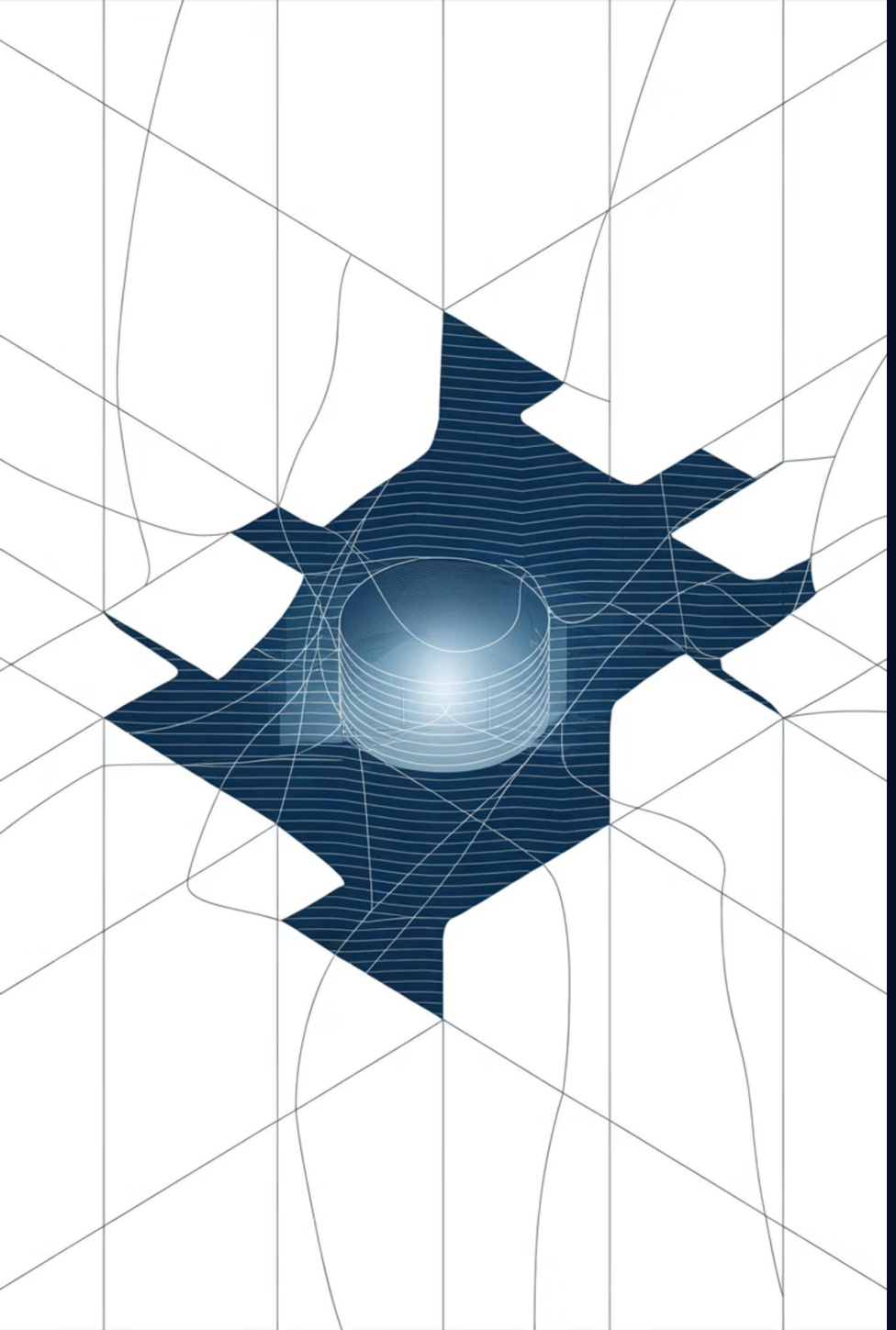


The Art of Concealment

CVE's Challenge with Transparency

Presented by Jerry Gamblin

About Me: Jerry Gamblin

I have a background in government, with a deep specialization in vulnerability management and the CVE community. As an active member, I participate in various working groups and am part of the EPSS Special Interest Group.

Government Background

Experienced in public sector security.

Vulnerability & CVE Expertise

Deep specialization in managing vulnerablity managment programs.

EPSS SIG Contributor

Active in advancing predictive vulnerability scoring.

Announcing the Launch of RogoLabs.net

RogoLabs Live!

We're officially launching RogoLabs, an initiative to tackle data quality challenges in our industry.

Focus on Quality

Shifting from just tracking quantity to measuring the **quality** and **completeness** of vulnerability data.

Expanding the RogoLabs Portfolio

In addition to RogoLabs.net, we're excited to launch two new community-focused projects:

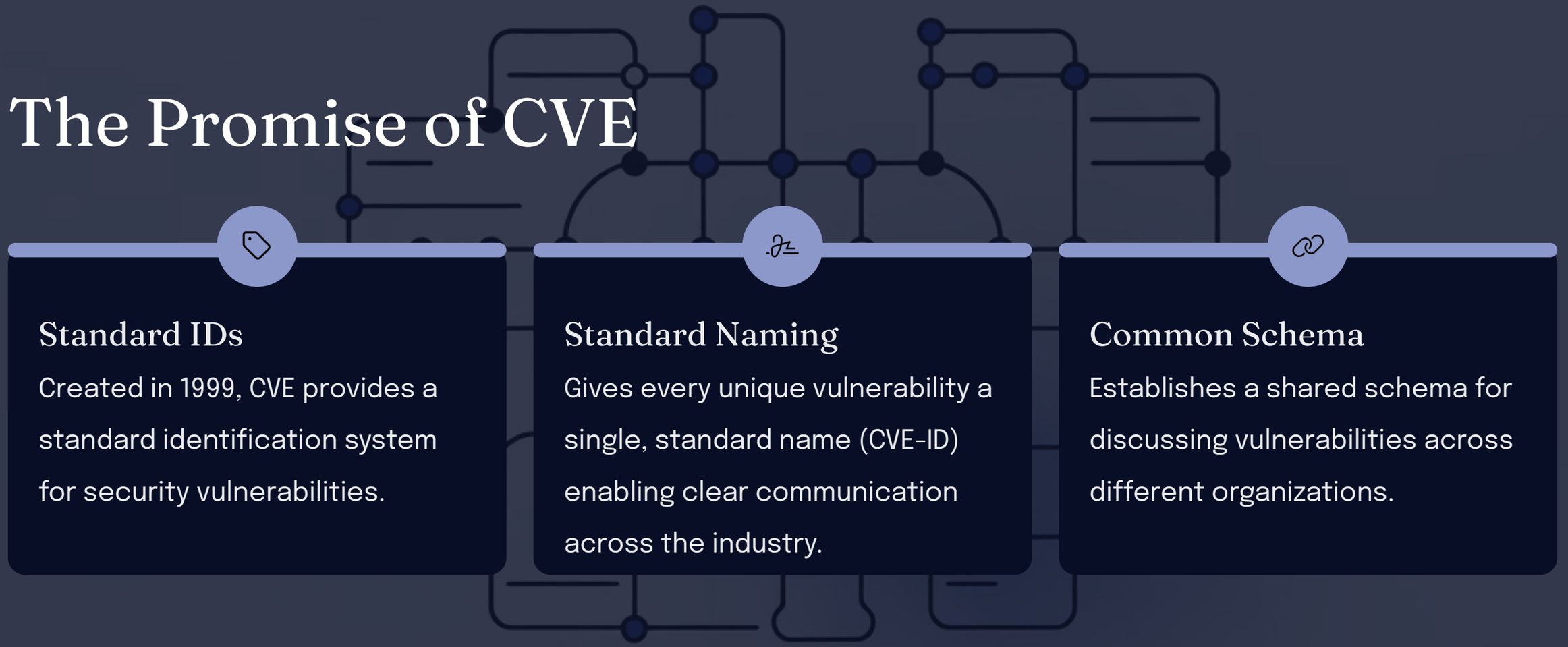
- CVE.icu
- CVEForecast.org

Open-Source & Community

All projects, including source code, will be on GitHub, fostering community-driven improvements.

Visit RogoLabs.net to explore our initiatives!

The Promise of CVE



Standard IDs

Created in 1999, CVE provides a standard identification system for security vulnerabilities.

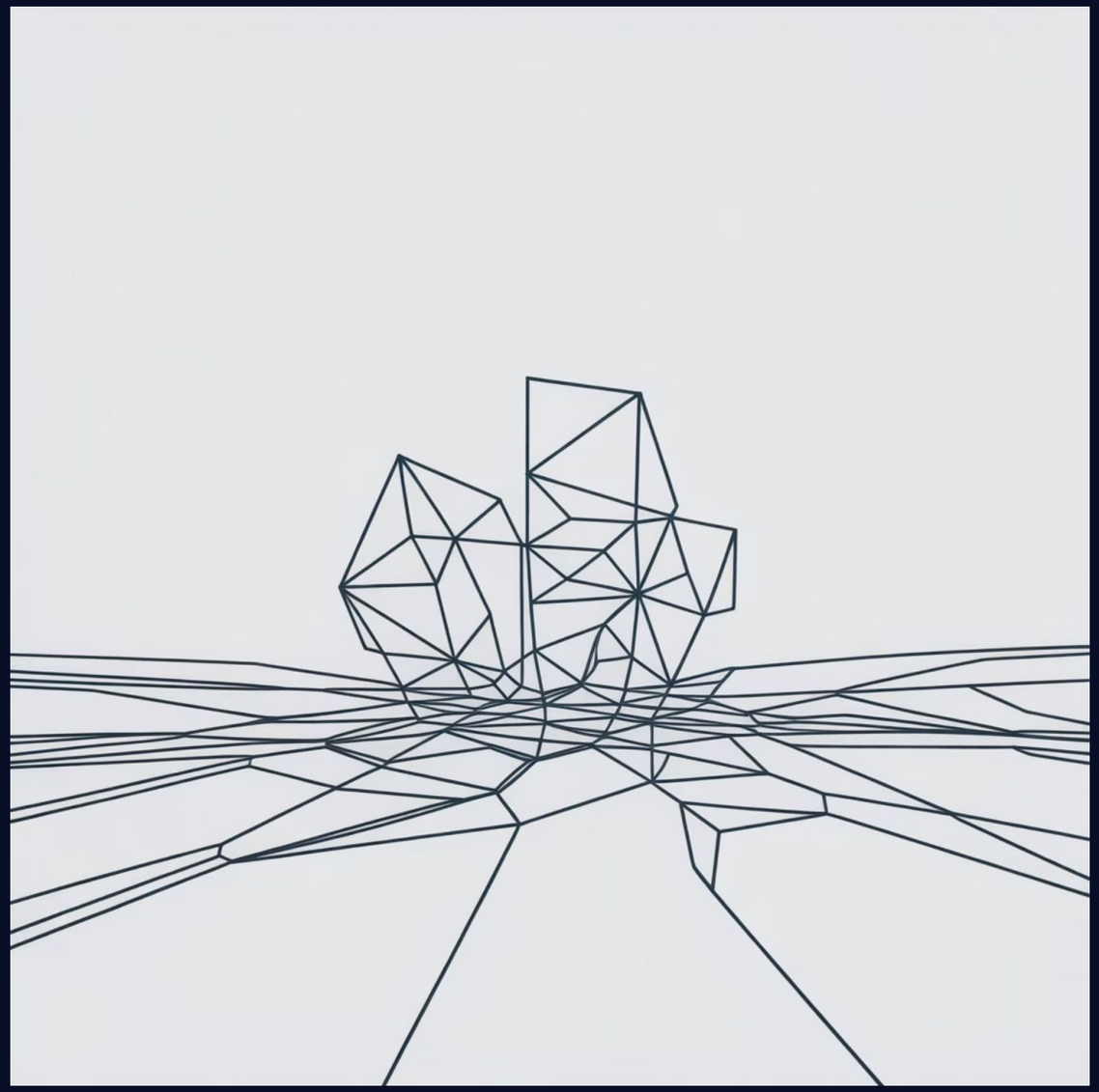
Standard Naming

Gives every unique vulnerability a single, standard name (CVE-ID) enabling clear communication across the industry.

Common Schema

Establishes a shared schema for discussing vulnerabilities across different organizations.

The Broken Promise



Incomplete Data

A growing percentage of CVE records are published with vague, incomplete, or missing details

Alert Fatigue

Security teams are forced to manually investigate alerts that lack context, leading to much slower response times.

Failed Automation

When CVE records lack key data, automated tools fail, creating dangerous blind spots

The Anatomy of an Actionable CVE

An actionable CVE requires a foundational level of completeness, but also builds upon four key pillars:

What kind of flaw?

The Weakness (CWE)

What's affected?

The Product (CPE)

How to fix it?

The Fix (Patch Info)

How severe?

The Severity (CVSS)

Even with foundational completeness, a CVE's value for security operations is significantly limited without details for these four pillars, making it incomplete for actionable intelligence.

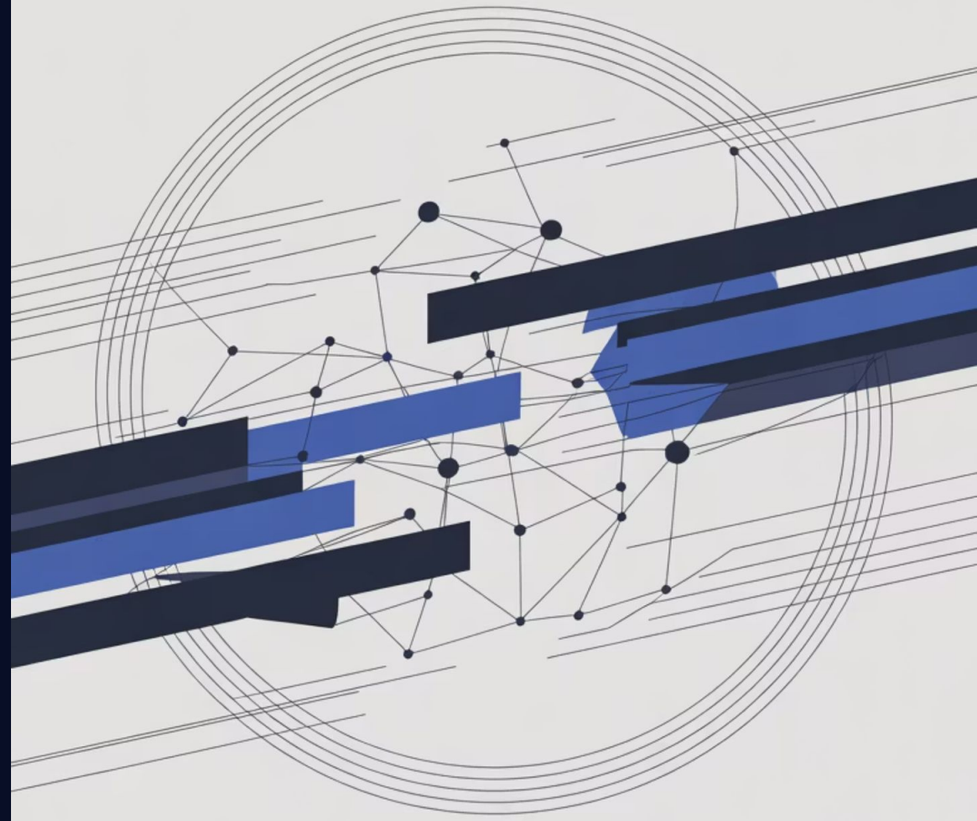
Pillar 1: The Weakness (CWE)

Common Weakness Enumeration

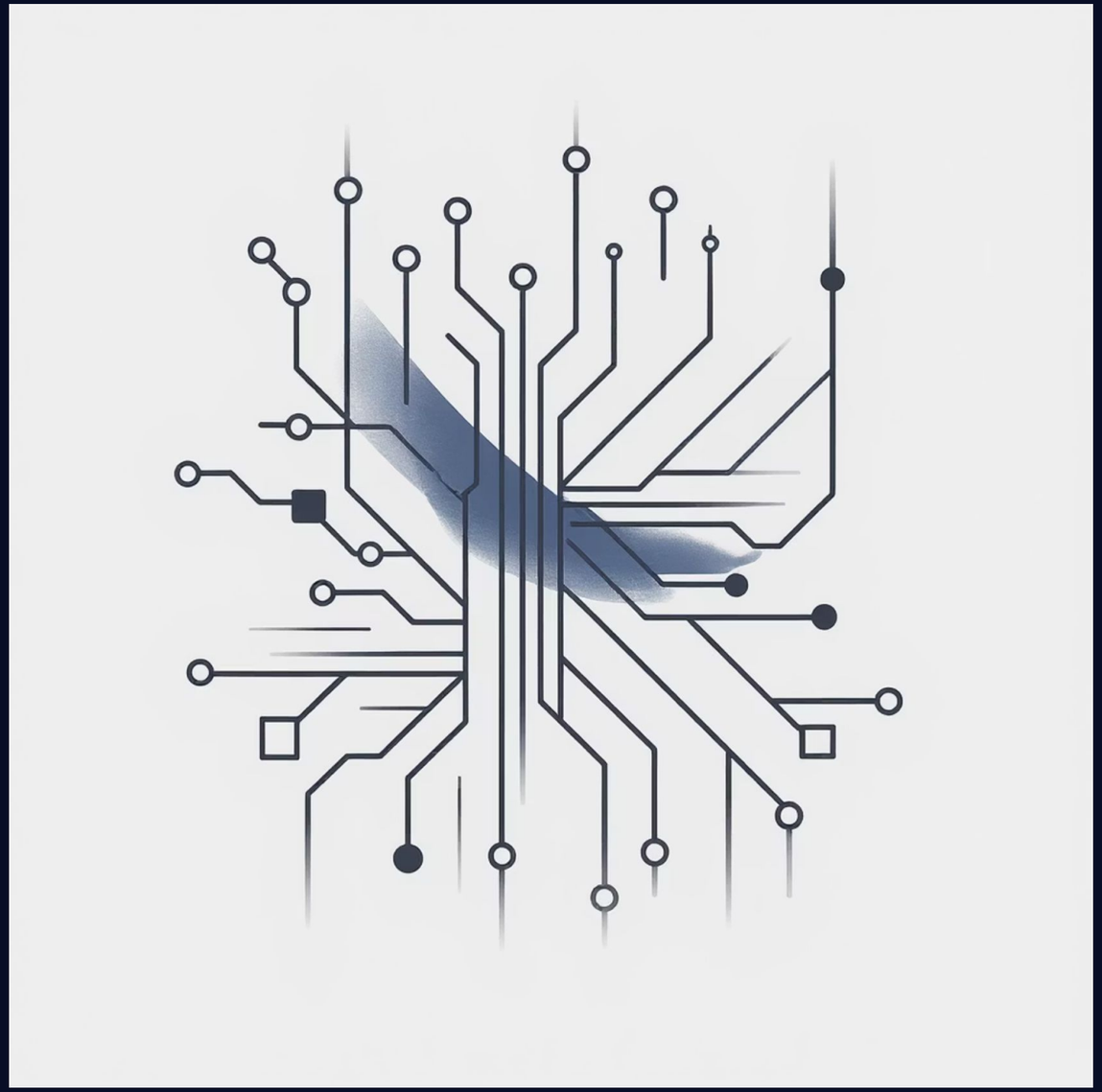
A dictionary of underlying software or hardware flaws that explains the root cause of vulnerabilities

- Examples: SQL Injection (CWE-89), Cross-site Scripting (CWE-79)
- Enables root cause analysis beyond fixing individual bugs
- Provides structured language for secure coding practices
- Helps developers eliminate entire classes of errors

CWE allows security teams to move from reactive bug-fixing to proactive secure development



Pillar 2: The Product (CPE)



Common Platform Enumeration

A standardized naming scheme for precisely identifying affected IT products

```
cpe:/a:apache:http_server:2.4.54
```

The Automation Key

Vulnerability scanners match CPEs on your network against CPEs in CVE records

Critical Failure Point

A CVE without a complete CPE is invisible to automated systems—creating a false sense of security

Pillar 3: The Severity (CVSS)

Common Vulnerability Scoring System (CVSS) is the primary mechanism security teams use to triage alerts and prioritize limited resources. It quantifies the severity of a vulnerability, enabling a consistent and standardized approach to risk assessment.

Understanding CVSS Scores

0.0-3.9

Low

Limited impact, typically requires local access

4.0-6.9

Medium

Moderate impact, may affect confidentiality, integrity, or availability

7.0-8.9

High

Significant impact, often remotely exploitable

9.0-10.0

Critical

Severe impact, easily exploitable, urgent remediation needed

Why CVSS Matters

Many organizations have SLAs and compliance requirements tied directly to CVSS ratings (e.g., "patch all Criticals within 15 days"). Without a clear CVSS score, prioritizing and managing vulnerabilities becomes a chaotic, manual process, leading to missed deadlines and increased risk.

CVSS provides a universal language for assessing vulnerability impact, crucial for efficient security operations.

Pillar 4: The Fix (Patch Info)

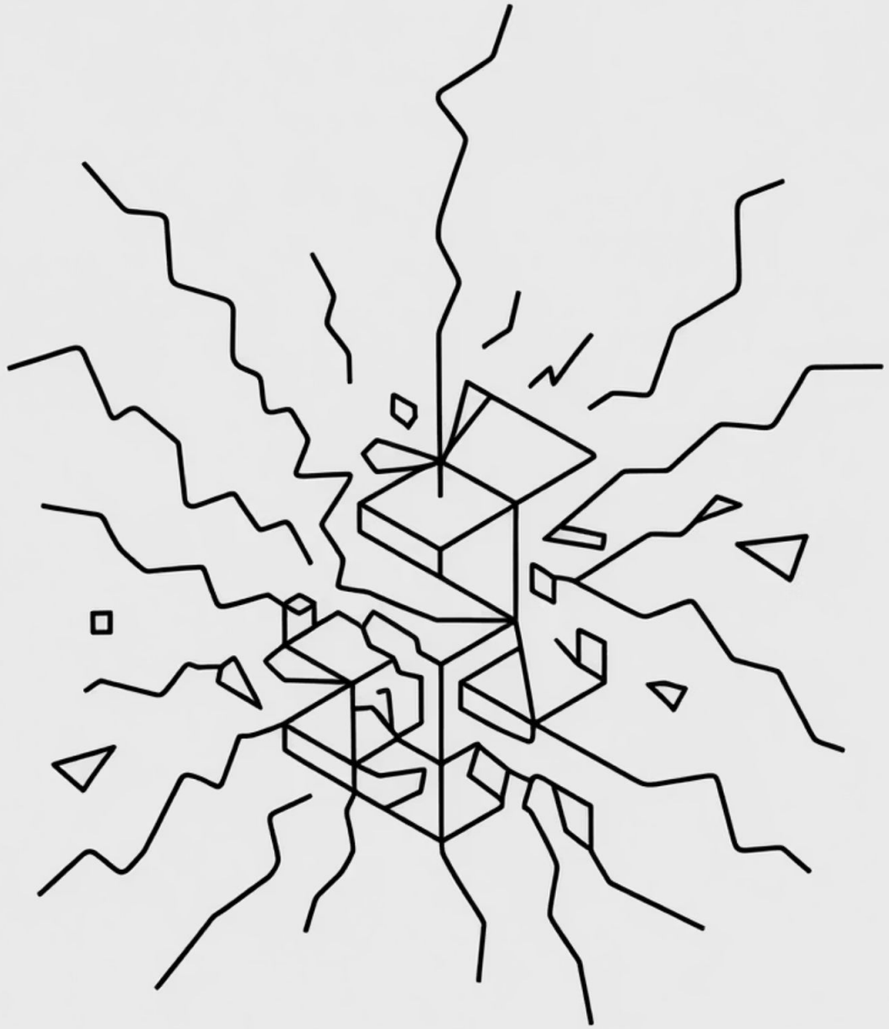
The Ultimate Goal

Vulnerability management is about remediation–a CVE record is incomplete without a clear path to a solution

What a "Fix" Looks Like

- Direct link to vendor security advisory
- Patch download information
- Specific code commit that resolves the flaw

⚠ A CVE that tells you you're vulnerable but doesn't tell you how to fix it is just a problem statement–generating work without providing solutions



The Reality: A System in Crisis

NVD Backlog

Since early 2024, thousands of CVEs have been left unanalyzed, without severity scores or product information

Systemic Failure

The backlog is a critical issue, but it's a symptom of a deeper problem: systemic failure of data enrichment at the source

Alarming Trend

In 2024 alone, over 14,000 CVEs were published without CPEs—more than the previous four years combined

Impact on Security Operations

Blind Spots

Vulnerabilities without CPEs can't be detected by scanners, creating security gaps

Increased Risk

Critical vulnerabilities go unpatched due to incomplete information

Wasted Time

Security teams spend hours manually researching vague CVEs to determine applicability

Resource Drain

Organizations hire specialists to compensate for incomplete data

The consequence: security programs become less effective, more expensive, and leave organizations exposed to preventable attacks.

The CNA Ecosystem Problem

A Federated Model

The CVE program scaled by delegating publishing authority to over 460 CNAs (CVE Numbering Authorities):

- Vendor
- Open Source
- Research
- Coordinator CNAs
- Hosted Services
- CNA-LR (CNA of Last Resort)
- Root and Top-Level Root (TL-Root)

Theory: Those closest to the vulnerability can provide the best data.

Misaligned Incentives

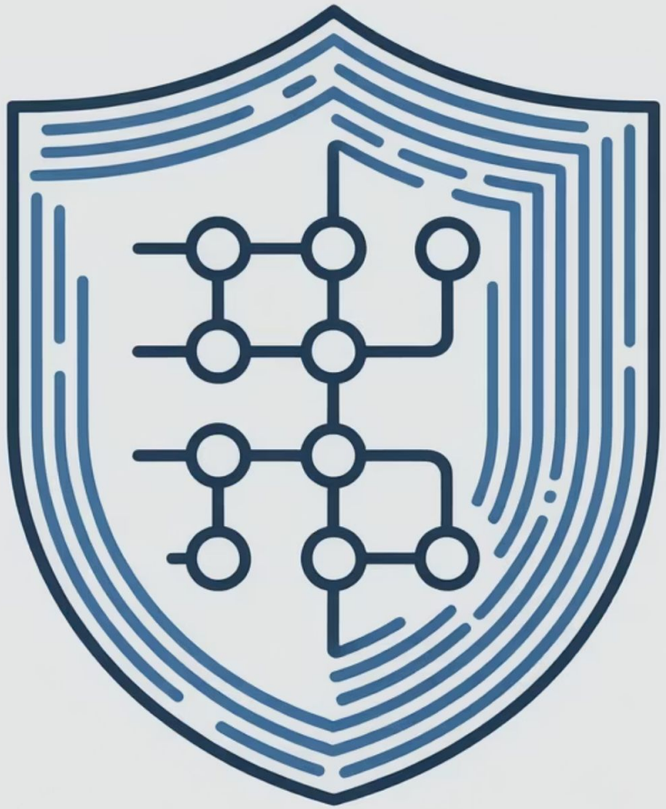
Few direct incentives for CNAs to publish complete, enriched records

Disincentives to Transparency

High CVSS scores can alarm customers; detailed technical information can aid attackers

Tragedy of the Commons

Without accountability, the path of least resistance is to publish minimal data



A Path Forward: We Can't Improve What We Don't Measure

Start with Measurement

Establish clear metrics for CVE data quality that can be consistently tracked

Create Accountability

Make CNA performance transparent and comparable through public reporting

Drive Improvement

Use data-backed metrics to encourage CNAs to improve their disclosure practices

Restore Trust

Rebuild confidence in the CVE ecosystem through demonstrated data quality

The Public Launch of CNAScoreCard.org

To tackle the data quality crisis, RogoLabs is launching CNAScoreCard.org

The first public, data-driven scorecard for every CVE Numbering Authority, providing objective measurement necessary to drive improvement across the entire ecosystem.

How CNAScoreCard.org Works

CWE Score

Does the record have a specific CWE identifier, or is it a generic placeholder?

CPE Score

Does the record contain one or more CPE strings with specific version information?

CVSS Score

Is a CVSS v3, v3.1 or v4.0 vector string and base score included?

Patch Score

Does the record contain a reference link explicitly tagged as a vendor-advisory or patch?

These component scores are aggregated to produce an overall quality score for each CVE, which are then rolled up to calculate a letter grade for each publishing CNA.

The CNA Scorecard in Action

Real-time Feed

Live stream of new CVEs, each with a completeness score and breakdown of its performance against the four pillars

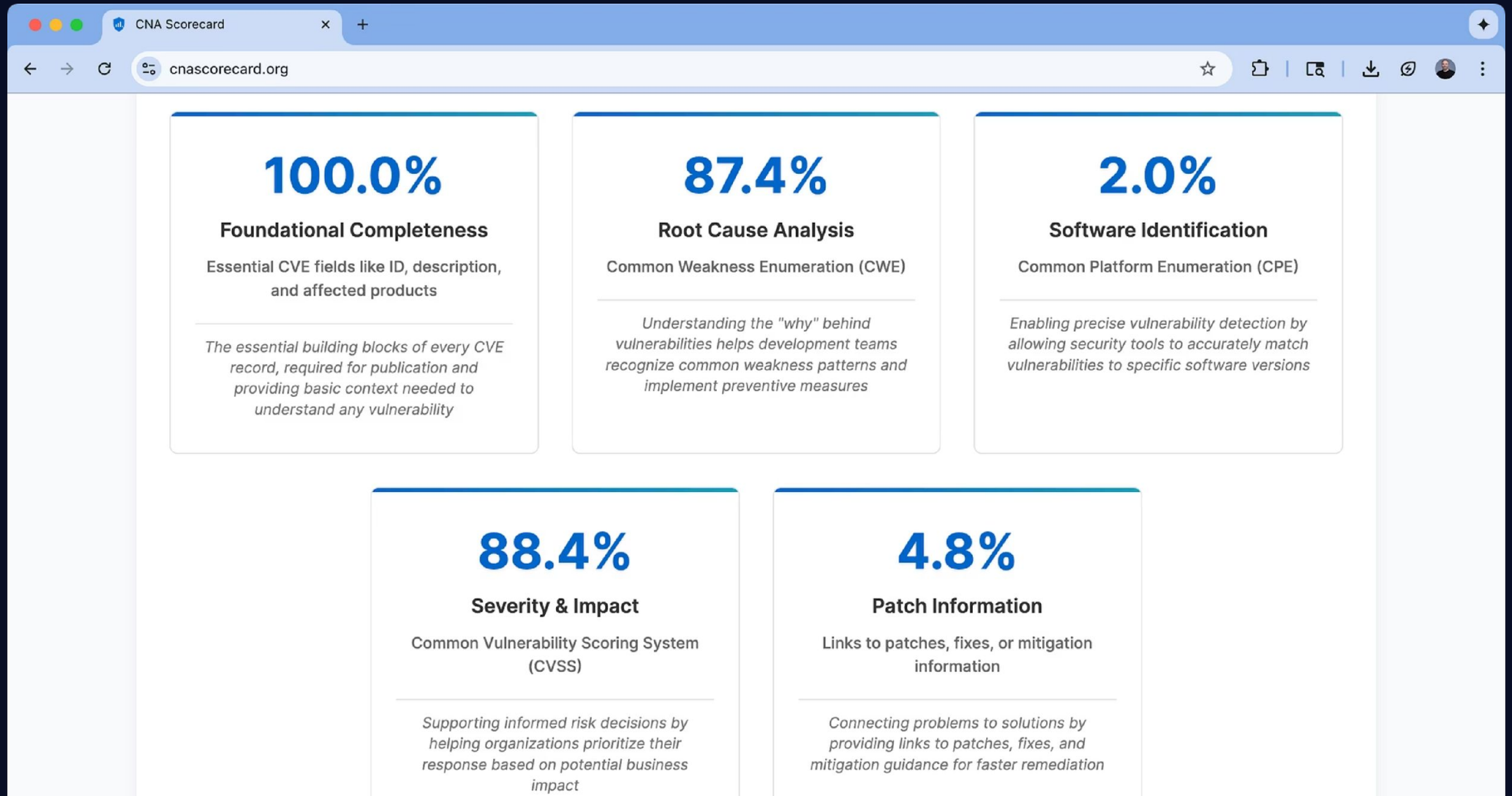
CNA Leaderboard

Ranks all 460+ CNAs based on the aggregate quality of their CVE records, creating healthy competition

Trend Analysis

Historical data showing improvement or degradation of data quality over time for individual CNAs and the ecosystem

The goal is to illuminate and encourage improvement, not to shame organizations.


CNA Scorecard
cnascorecard.org
100.0%
Foundational Completeness
Essential CVE fields like ID, description, and affected products
The essential building blocks of every CVE record, required for publication and providing basic context needed to understand any vulnerability
87.4%
Root Cause Analysis
Common Weakness Enumeration (CWE)
Understanding the "why" behind vulnerabilities helps development teams recognize common weakness patterns and implement preventive measures
2.0%
Software Identification
Common Platform Enumeration (CPE)
Enabling precise vulnerability detection by allowing security tools to accurately match vulnerabilities to specific software versions
88.4%
Severity & Impact
Common Vulnerability Scoring System (CVSS)
Supporting informed risk decisions by helping organizations prioritize their response based on potential business impact
4.8%
Patch Information
Links to patches, fixes, or mitigation information
Connecting problems to solutions by providing links to patches, fixes, and mitigation guidance for faster remediation

How This Helps the Community

For Defenders

Use completeness scores to filter intake and prioritize actionable CVEs; use CNA grades as a trust metric for vendors

For CNAs

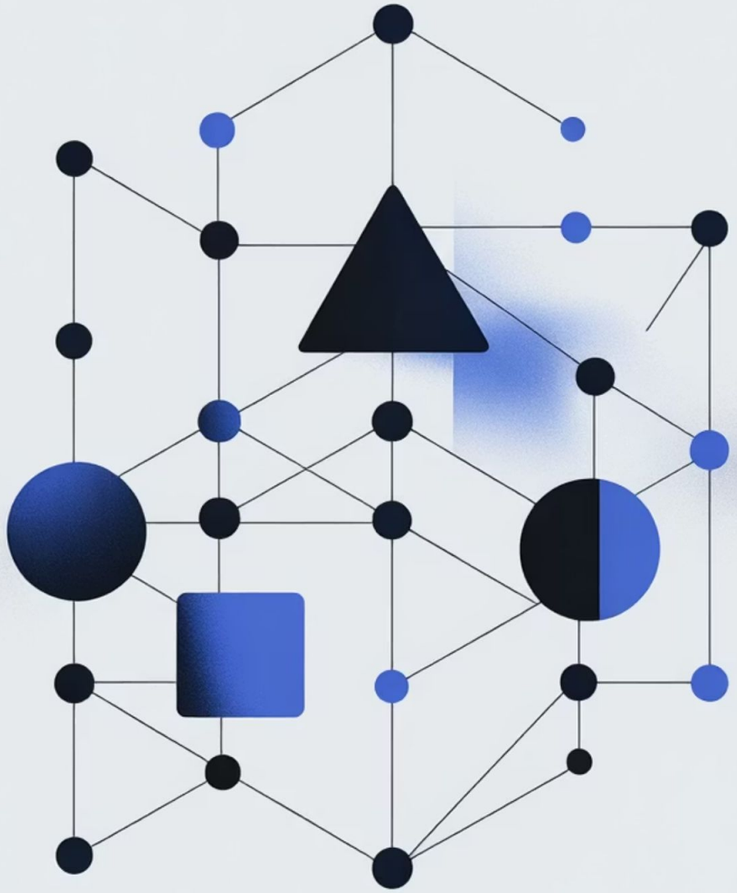
Get clear benchmarks to measure disclosure processes against peers and identify specific areas for improvement

For the Ecosystem

Establish a public, continuously updated metric for the health of CVE data, creating needed accountability

For Compliance

Provide objective evidence for regulatory discussions about vendor security practices and transparency



Call to Action

For Security Practitioners

Use the tool. Visit **CNAScoreCard.org**. When a vendor gives you an incomplete CVE, use the scorecard as evidence to demand better data.

For CNAs

Review your organization's score. If it's not an 'A', treat it as a roadmap for improvement. High-quality disclosure builds customer trust.

For Everyone

This is an open-source project hosted at RogoLabs.net. Get involved. Help us improve the scoring logic. Let's fix this together.

Conclusion & Key Takeaways

The Problem

The CVE system is drowning in incomplete data, breaking automated tools that modern security programs depend on

The Standard

An actionable CVE must have all four pillars:

Defined **Weakness (CWE)**

Identified **Product (CPE)**

Calculated **Severity (CVSS)**

Clear **Fix (Patch)**

The Solution

CNAScoreCard.org provides the transparency and data-driven accountability needed to drive improvement

Contact Information

Jerry Gamblin

- @JGamblin
- rogolabs.net
- CNAScoreCard.org
- CVE.icu

Let's work together to restore the promise of a truly common and actionable language for vulnerability management.