# A Bigger Map Is Not a Bigger Territory

Retiring the vulnpocalypse before AI-scale discovery arrives

**Jerry Gamblin** . **RogoLabs**

CVE in an Era of AI-Enabled Vulnerability Discovery . 30 July 2026

JANUARY 1999 . PURDUE UNIVERSITY

# This Has Always Been a Naming Program

David Mann and Steve Christey, MITRE, presented "Towards a Common Enumeration of Vulnerabilities."

The problem was never too many vulnerabilities. It was too many names for the same one:

> *"There is no common naming convention and no common enumeration of the vulnerabilities in these disparate databases."*

We built a global institution because agreeing on what to call a thing was worth it.

**We have a second naming problem now.**
**This one we gave ourselves.**

**321**
**CVE ENTRIES AT LAUNCH**
September 1999

**353,000+**
**CVE RECORDS TODAY**
533 CNAs across 43 countries

Mann & Christey, Purdue, Jan 1999. Launch count: cve.org. Records: cvelistV5. CNAs: CVE Program CNA list. All as of 28 July 2026.

SPECIMENS . 2026

# The Words We Use for Our Own Success

**"The vulnpocalypse has begun."**

Jessica Lyons, The Register, May 2026

**"...the 'tsunami' that is coming towards us"**

Chris Gibson, CEO of FIRST, Infosecurity Magazine, Apr 2026

**"The Vulnerability Tsunami"**

Trinity Cyber, July 2026

**"...the superlatives are warranted"**

Rich Mogull, CSA, Apr 2026 (a skeptic)

**Full disclosure: I count these at cve.icu. I co-author the mid-year CVE forecast at FIRST. That scary number people call a flood? I helped build it.**

**Counting is not the problem. Turning the count into an apocalypse is.**

CVE®

THE EVIDENCE, PART ONE

# Change One Word. Watch the Decision Change.

## 47% → 31%

**chose surgery for the identical diagnosis**

394 women, one low-risk diagnosis, the same stated risks. Called "noninvasive breast cancer," 47% chose surgery. Called "abnormal cells," 31% did.

The National Cancer Institute went further, and recommended taking the word "cancer" out of these diagnoses entirely.

**And in Public Health**

The WHO writes formal rules for naming diseases, to avoid names that

**"incite undue fear"**

and that create "unjustified barriers to travel, commerce and trade."

**A bad name changes what people do.**

Omer et al., JAMA Internal Medicine, 2013 (N=394). Esserman et al., JAMA, 2013. WHO news release on naming new human infectious diseases, 8 May 2015.

THE EVIDENCE, PART TWO

# Finding More Is Not the Same as There Being More

### South Korea, Thyroid Cancer

Ultrasound screening spread. Diagnoses rose 15 times in 18 years. Deaths never moved.

The harm was never the finding. Nearly everyone diagnosed got surgery, and two thirds lost the whole thyroid.

**Then surgeries fell a third. Deaths still never moved.**

### Epidemiology Has a Word for This

**an ascertainment artifact**

The word exists so nobody mistakes the map for the territory.

## A Bigger Map Is Not a Bigger Territory.

More CVEs mean more visibility into risk that already existed. Keep reporting. Finding and fixing are two different decisions.

Ahn, Kim, Welch, "Korea's Thyroid-Cancer Epidemic," NEJM 2014; follow-up "Turning the Tide," NEJM 2015.

EVIDENCE, FROM OUR OWN FIELD

# We Have Already Proved Naming Moves Us

## Heartbleed, 2014

The bug that made branded vulnerabilities normal: a name, a logo, a website, a press strategy. Pew found 60% of US adults had heard of it.

The top of the web patched inside 48 hours. The tail never really did.

**A good name is a lever.**

## Badlock, 2016

A name, a logo, and a countdown site three weeks before the bug was disclosed. The brand arrived before the vulnerability did.

Trustwave's verdict: it did not "rise to any level that deserves the focus."

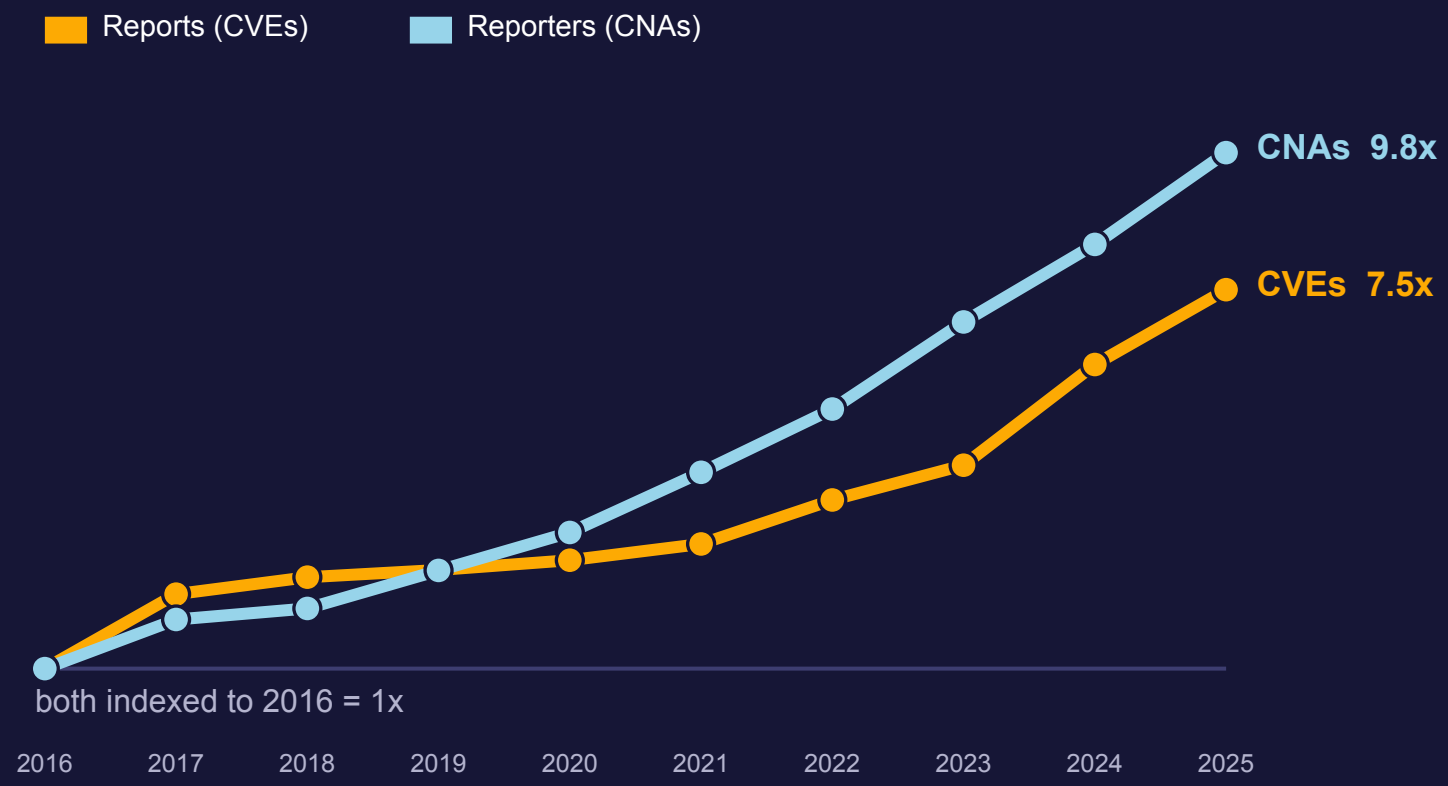
**The same lever, aimed at fear.**

**A name is a tool. We can point it at prioritization, or at panic. "Vulnpocalypse" points it at panic.**

Heartbleed: CVE-2014-0160. Awareness: Pew, Apr 2014. Patch rates: Durumeric et al., IMC 2014. Badlock: CVE-2016-2118, disclosed 12 Apr 2016; criticism: Trustwave.

WHAT ACTUALLY GREW

# More Reporters, Not More Risk




**Output per reporter**

## 24% lower

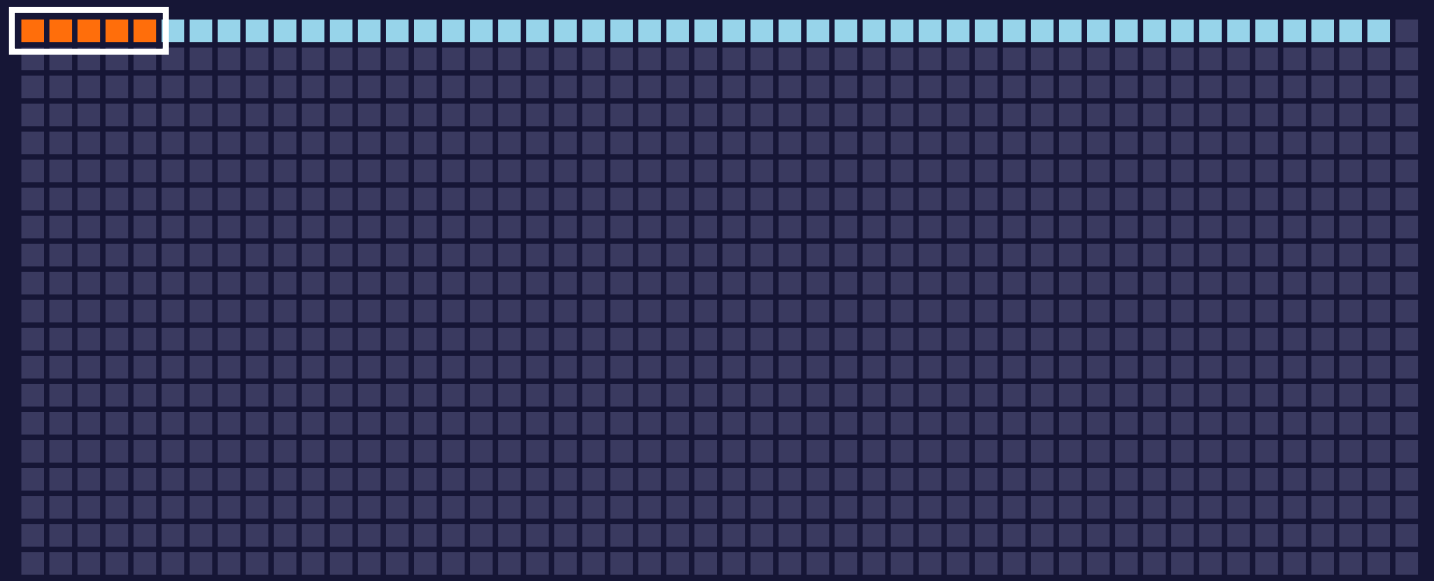
Program-wide, CVEs per active CNA fell from 174 to 133 as participation broadened. The map got bigger. The territory did not.

Being honest: annualize 2026 and per-reporter output ticks back up. That is the AI signal arriving, coverage continuing, not a disaster.

cve.icu, active CNAs vs published CVEs, 2016 to 2025 full years.

RAW COUNTS WERE NEVER THE UNIT OF WORK

# 1,000 Squares. Every Published CVE.



In CISA KEV

**1 in 213**

lands on CISA's KEV list.

EPSS > 0.1

**1 in 20**

scores high enough to watch.

We already have magnitude scales: Richter 1935, Fujita 1971, Saffir and Simpson in the early 1970s. Nobody says they cannot keep up with earthquakes.

**EPSS, KEV, and SSVC are ours. Volume is not workload.**

Two lenses, one story: the actionable slice is small, and neither lens is the raw count.

Same denominator: EPSS now scores 99.98% of published records.

1,655 of 353,273 published records in CISA KEV (catalog 2026-07-27); 17,254 score EPSS > 0.1 (2026-07-28). KEV is a curated list, not a measured rate; EPSS > 0.1 is a practitioner convention, not a standard.

THE COST

# Who Pays for the Doom Vocabulary

### Leaders

read the growth curve as failure, when it shows the program working, even through a hard two years.

### CNAs & Vendors

learn that every record they publish adds to "the problem." That is a reason not to disclose.

### Defenders

hear "you cannot keep up" and reasonably stop trying. Burnout and checkbox compliance follow.

### And the Y2K Cost

The world spent around $300 billion. Almost nothing broke, so the public decided it had been a hoax. Cry apocalypse and survive it, and you do not get credit for the save. You lose the room the next time.

Y2K spend: estimates on the order of $300 billion worldwide (U.S. Senate Y2K Committee final report, 2000, citing IDC).

THE TAKEAWAY

# Four Words to Change Before the Next Curve

| RETIRE | | REPLACE WITH |
|---|---|---|
| "vulnpocalypse" | → | retire it. It never described anything. |
| "the CVE flood" | → | coverage growth |
| "keeping up with CVEs" | → | prioritizing from CVEs |
| "drowning in vulnerabilities" | → | we can finally see the risk that was always there |

*Or the way I say it on my own site: AI is bringing the rain, not the flood.*

# Stop Grading the Catalog by Its Size.
# Measure the Gap Between Exploitation and Remediation.

I will keep counting, and keep forecasting. That part is the job. AI scales discovery, and it scales triage at the same time. The publication rate is about to look absurd, and it will not matter, because publication rate was never the number.

***A Bigger Map Is Not a Bigger Territory.***

Jerry Gamblin . RogoLabs . github.com/jgamblin . jerry.gamblin@gmail.com

BACKUP . FOR Q&A

# CVEs per Active CNA, in Full

## The mean, and the median

Mean CVEs per active CNA: 174 in 2016, 133 in 2025. Down about 24%.

**Median: 40 in 2016, 10 in 2025. Down 75%.**

The median is the stronger claim. Typical CNAs got smaller, not busier.

## The honest caveat

The mean is skewed by a few very large issuers, MITRE most of all. So do not read 174 to 133 as "the typical CNA."

Concentration fell too: the largest single CNA was 25.5% of all records in 2016 and 14.5% in 2025.

**The robust claim: total CVEs x7.5, active CNAs x9.8, 2016 to 2025. The gap between those two is the point, not the ratio.**

cvelistV5 and cve.icu: active CNAs vs published CVEs, 2016 to 2025 full years, as of 28 July 2026.

BACKUP . FOR Q&A

# The Real Quality Caveat

## What improved

2026 records, CNA container only: 85% CVSS, 85% CWE. Counting ADP enrichment as well: 99.8% CVSS, 97.2% CWE.

CVSS v4 adoption climbing: 3,567 records in 2024, 12,419 in 2025.

## What declined

NVD enrichment. CPE coverage: ~100% through 2023, then 81% (2024), 63% (2025), 56% (2026 to date).

The newest month always undercounts: July 2026 records are only about 30% enriched so far. This is lag, not a quality regression.

**Honest framing: coverage of records grew; downstream enrichment is a separate, real problem. I do not conflate them.**

cvelistV5 (CNA and ADP containers) and NVD enrichment data, as of 28 July 2026.