Exploring 3,000+ Know Exploited Vulnerabilities

Patrick Garrity
(Security Researcher)

VulnCheck

PATRICKMGARRITY

SECURITY RESEARCHER

VulnCheck

DUO SECURITY

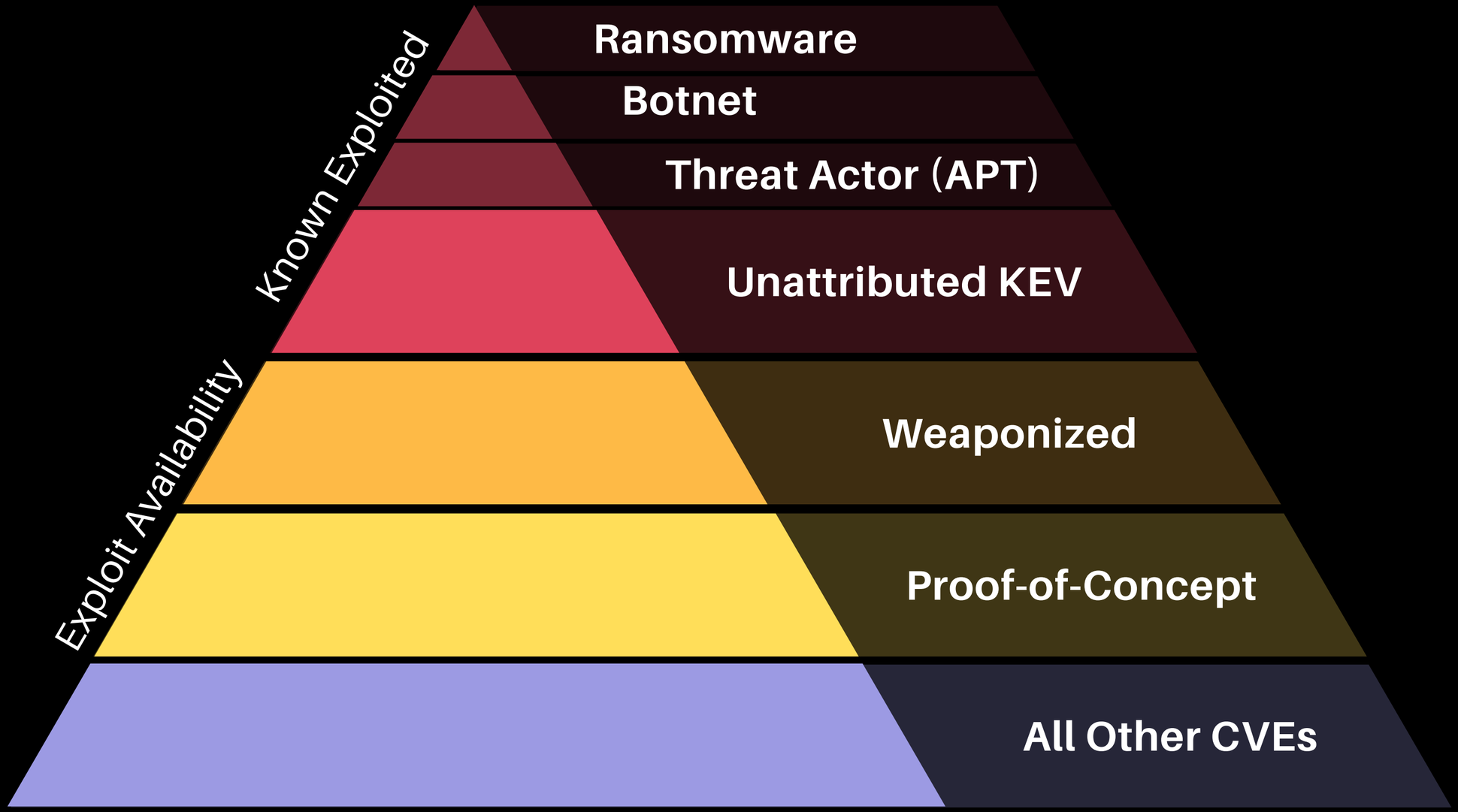
Nucleus

censys

Blumira

How do we improve prediction?

Where does KEV live?



VulnCheck

What is VulnCheck KEV?

We include any vulnerability publicly-reported as exploited in the wild in VulnCheck KEV.

Trusted Sources
Automated KEV

Everything else we collect is Analyzed by a human

Let’s Look At a Known Exploited Vulnerability…

JSON... Machine Readable


```
"data": [
  {
    "vendorProject": "DrayTek",
    "product": "Multiple Vigor Routers",
    "shortDescription": "DrayTek Vigor3900, Vigor2960, and Vigor300B devices contain an OS command injection vulnerability in cgi-bin/mainfunction.cgi/cvmcfgupload that allows for remote code execution via shell metacharacters in a filename when the text/x-python-script content type is used.",
    "vulnerabilityName": "DrayTek Multiple Vigor Routers OS Command Injection Vulnerability",
    "required_action": "Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.",
    "knownRansomwareCampaignUse": "Unknown",
    "cve": [
      "CVE-2020-15415"
    ],
    "vulncheck_xdb": [

    ],
    "vulncheck_reported_exploitation": [
      {
        "url": "https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json",
        "date_added": "2024-09-30T00:00:00Z"
      },
      {
        "url": "https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2024-02-01&host_type=src&vulnerability=cve-2020-15415",
        "date_added": "2024-02-01T00:00:00Z"
      },
      {
        "url": "https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2024-03-13&host_type=src&vulnerability=cve-2020-15415",
        "date_added": "2024-03-13T00:00:00Z"
      },
      {
        "url": "https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2024-03-14&host_type=src&vulnerability=cve-2020-15415",
        "date_added": "2024-03-14T00:00:00Z"
      },
      {
        "url": "https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2024-03-20&host_type=src&vulnerability=cve-2020-15415",
        "date_added": "2024-03-20T00:00:00Z"
      },
      {
        "url": "https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2024-03-21&host_type=src&vulnerability=cve-2020-15415",
        "date_added": "2024-03-21T00:00:00Z"
      },
      {
        "url": "https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2024-05-15&host_type=src&vulnerability=cve-2020-15415",
        "date_added": "2024-05-15T00:00:00Z"
      },
      {
        "url": "https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2024-08-28&host_type=src&vulnerability=cve-2020-15415",
        "date_added": "2024-08-28T00:00:00Z"
      },
      {
        "url": "https://dashboard.shadowserver.org/statistics/honeypot/vulnerability/map/?day=2024-09-14&host_type=src&vulnerability=cve-2020-15415",
        "date_added": "2024-09-14T00:00:00Z"
      },
      {
        "url": "https://unit42.paloaltonetworks.com/mirai-variant-v3g4/",
        "date_added": "2023-02-15T00:00:00Z"
      },
      {
        "url": "https://media.defense.gov/2024/Sep/18/2003547016/-1/-1/0/CSA-PRC-LINKED-ACTORS-BOTNET.PDF",
        "date_added": "2024-09-18T00:00:00Z"
      }
    ],
    "dueDate": "2024-10-21T00:00:00Z",
    "cisa_date_added": "2024-09-30T00:00:00Z",
    "date_added": "2023-02-15T00:00:00Z",
    "_timestamp": "2024-09-30T16:25:20.108623Z"
  }
```

VULNCHECK KEV EXPLOITATION TIMELINE

CVE-2020-15415 | DRAYTEK

2023-02-15

Exploitation Confirmed

Source: Palo Alto Networks
Mirai Variant V3G4 Targets
IoT Devices
Added to VulnCheck KEV

2024-02-01

Exploitation Activity First Seen*

Source: ShadowServer
Tag: 2023-03-01

2024-09-18

PRC Botnet Report

Source: Five Eyes

2024-09-30

Exploitation Confirmed

Source: CISA

VulnCheck

VULNERABILITIES

Mirai Variant V3G4 Targets IoT Devices

UNIT 42®
BY PALO ALTO NETWORKS

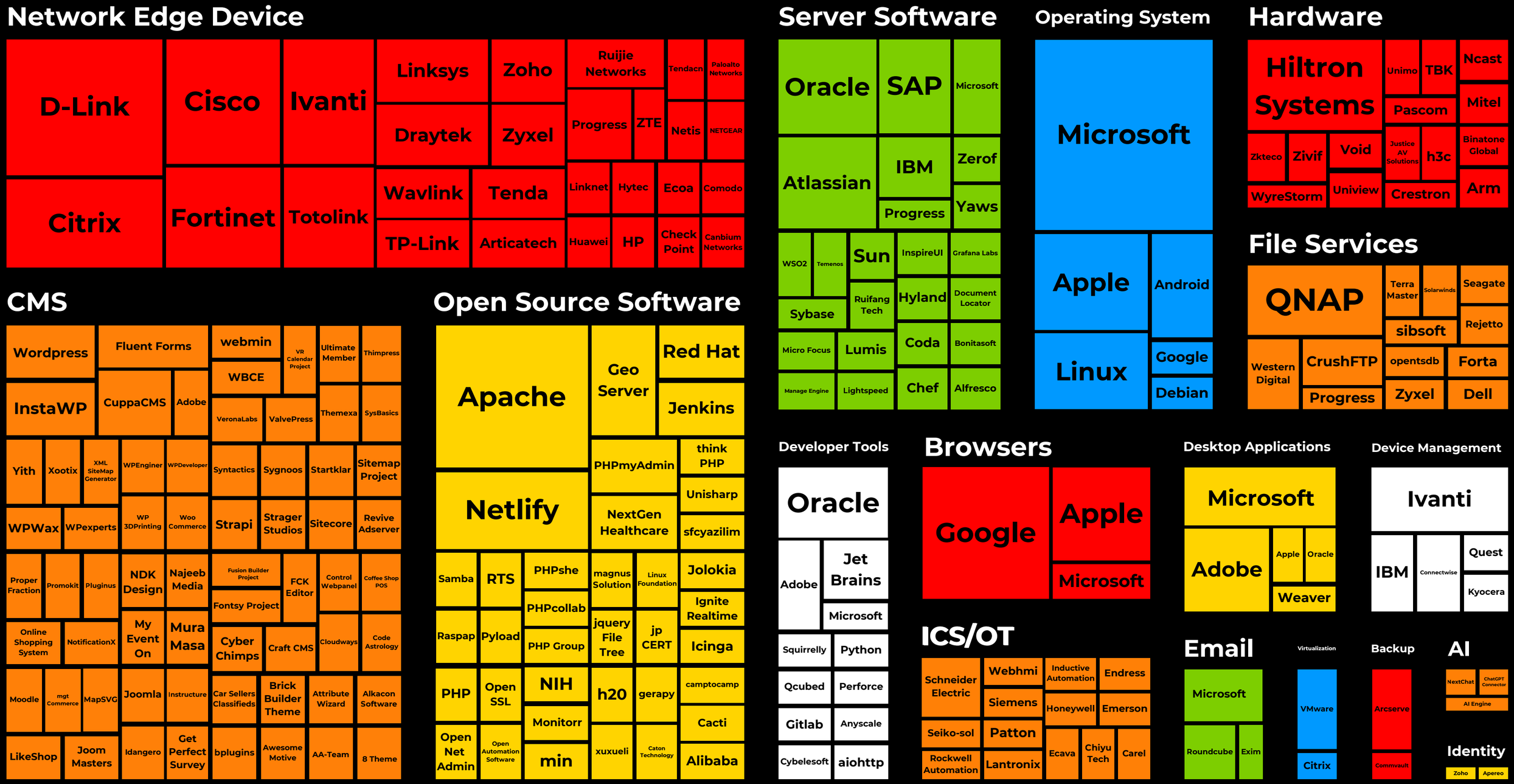
Executive Summary

From July to December 2022, Unit 42 researchers observed a Mirai variant called V3G4, which was leveraging several vulnerabilities to spread itself. The vulnerabilities exploited include the following:

- **CVE-2012-4869**: FreePBX Elastix Remote Command Execution Vulnerability
- **Gitorious Remote Command Execution Vulnerability**
- **CVE-2014-9727**: FRITZ!Box Webcam Remote Command Execution Vulnerability
- **Mitel AWC Remote Command Execution Vulnerability**
- **CVE-2017-5173**: Geutebruck IP Cameras Remote Command Execution Vulnerability
- **CVE-2019-15107**: Webmin Command Injection Vulnerability
- **Spree Commerce Arbitrary Command Execution Vulnerability**
- **FLIR Thermal Camera Remote Command Execution Vulnerability**
- **CVE-2020-8515:** DrayTek Vigor Remote Command Execution Vulnerability
- **CVE-2020-15415**: DrayTek Vigor Remote Command Injection Vulnerability

What Technologies Have Known Exploited Vulnerabilities?

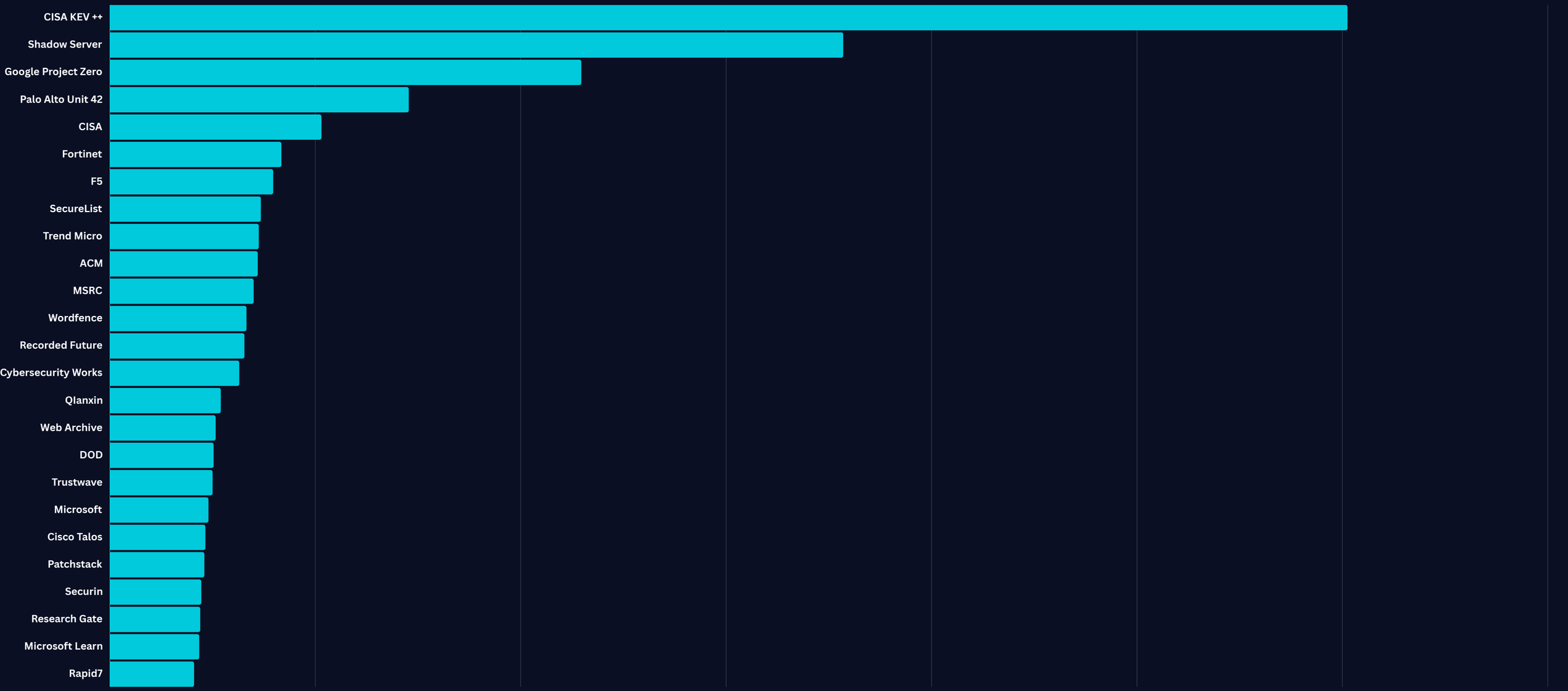
What Types of Technologie Have Known Exploited Vulnerabilties (1H-2024)



Who Reports KEVs?

Top 25 Sources for KEV by Unique CVE

Source: VulnCheck KEV

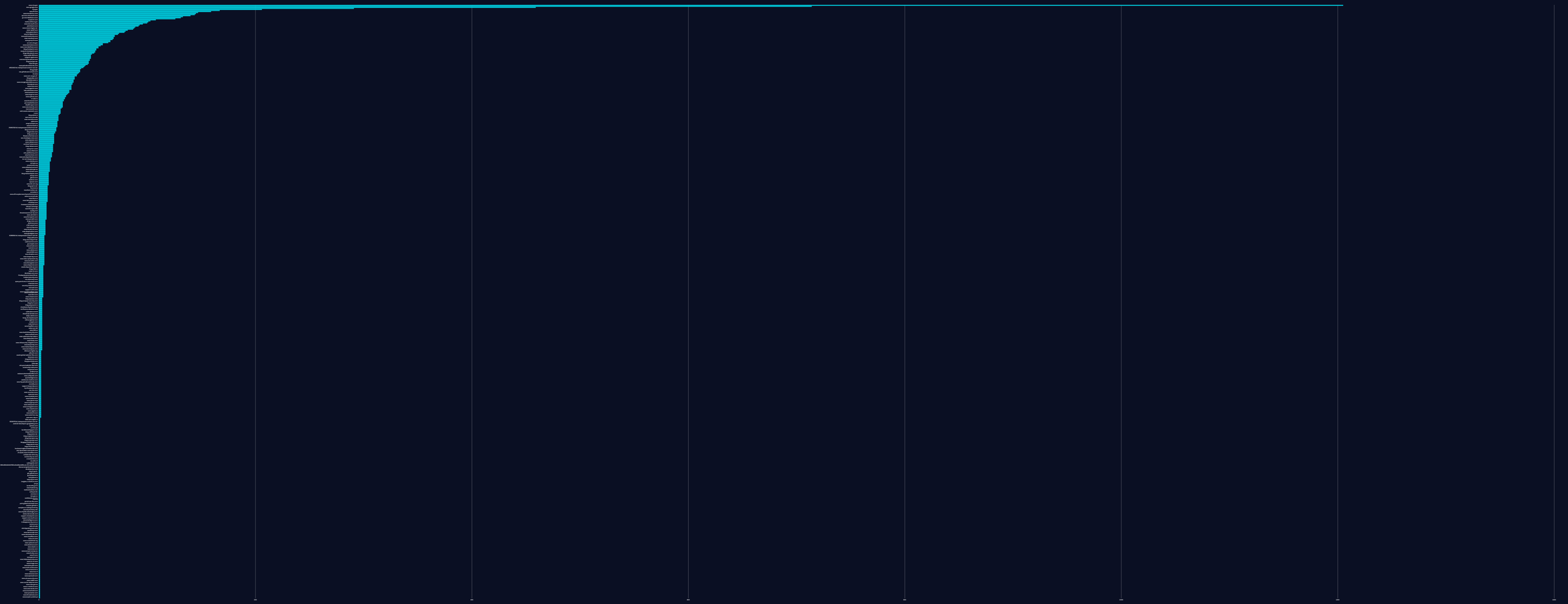


Year CVE Published

VulnCheck

All Sources for KEV by Unique CVE

500+ Source: VulnCheck KEV



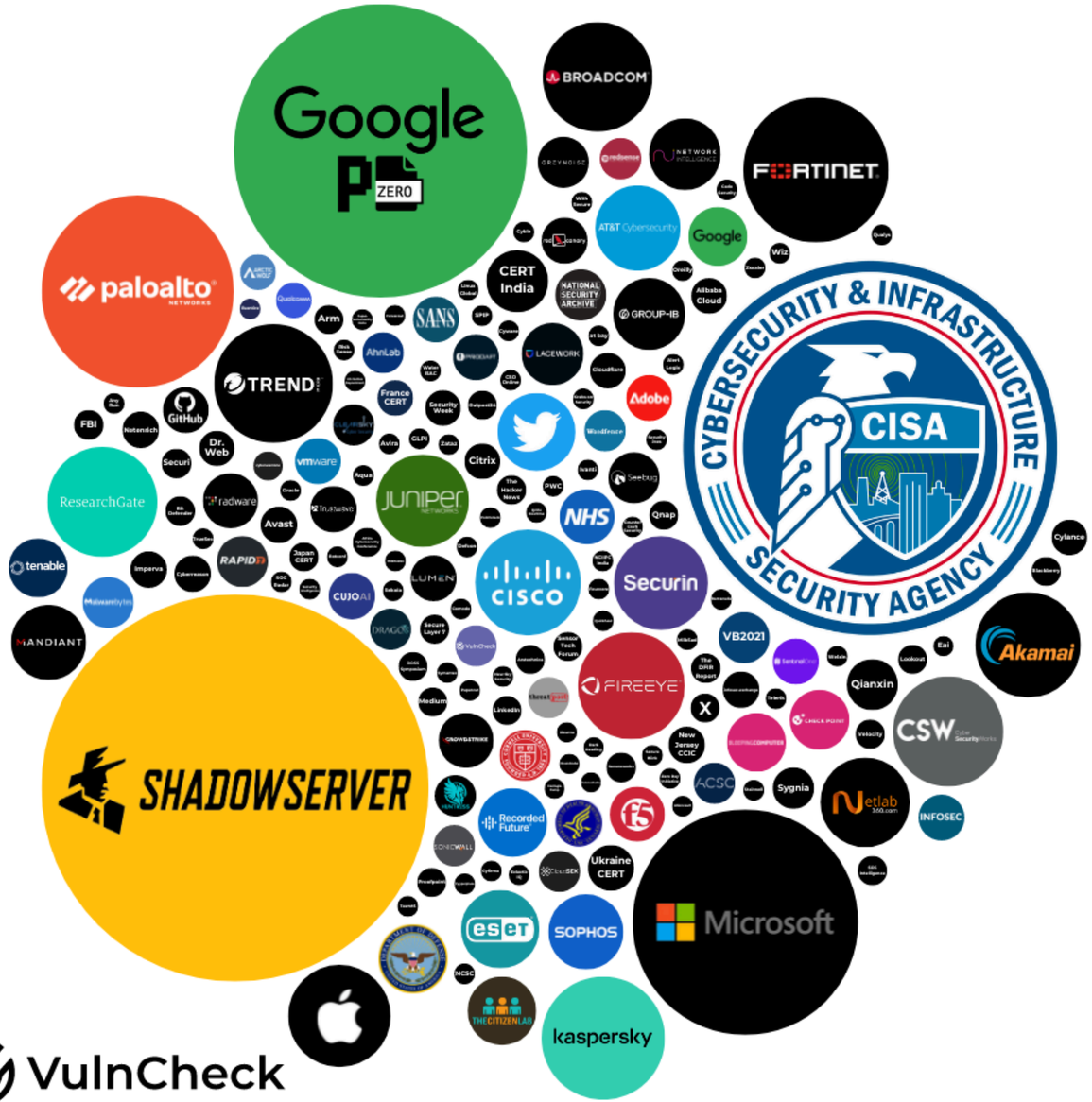
Year CVE Published

VulnCheck

Who Reports KEVs First?

Earliest Reporter of Exploitation in the Wild

Source: VulnCheck KEV (1965 Vulns over 20+ Years)

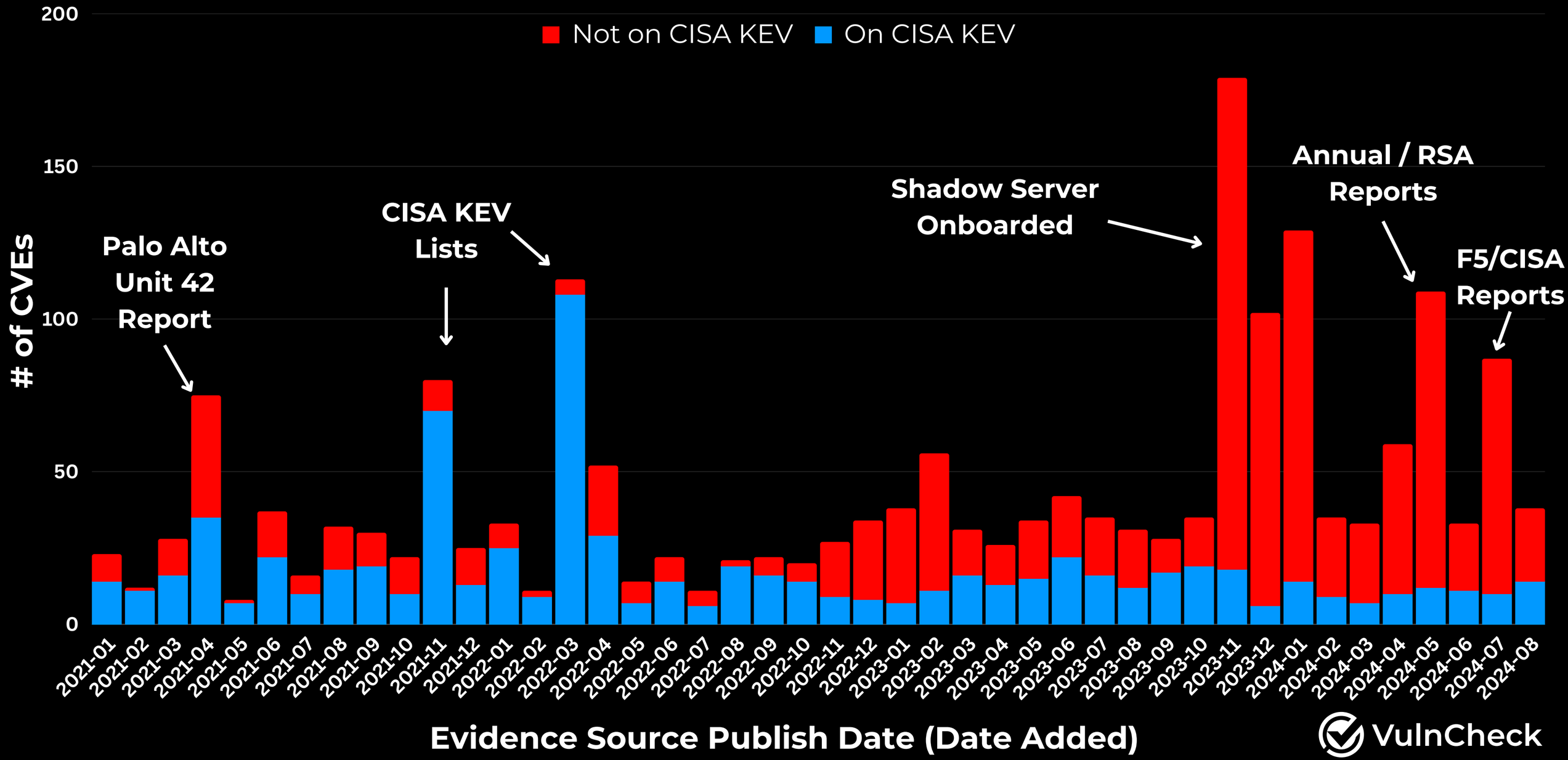


VulnCheck

Could KEVs be Forecasted?

Known Exploited Vulnerabilities (KEV)

Source: VulnCheck KEV

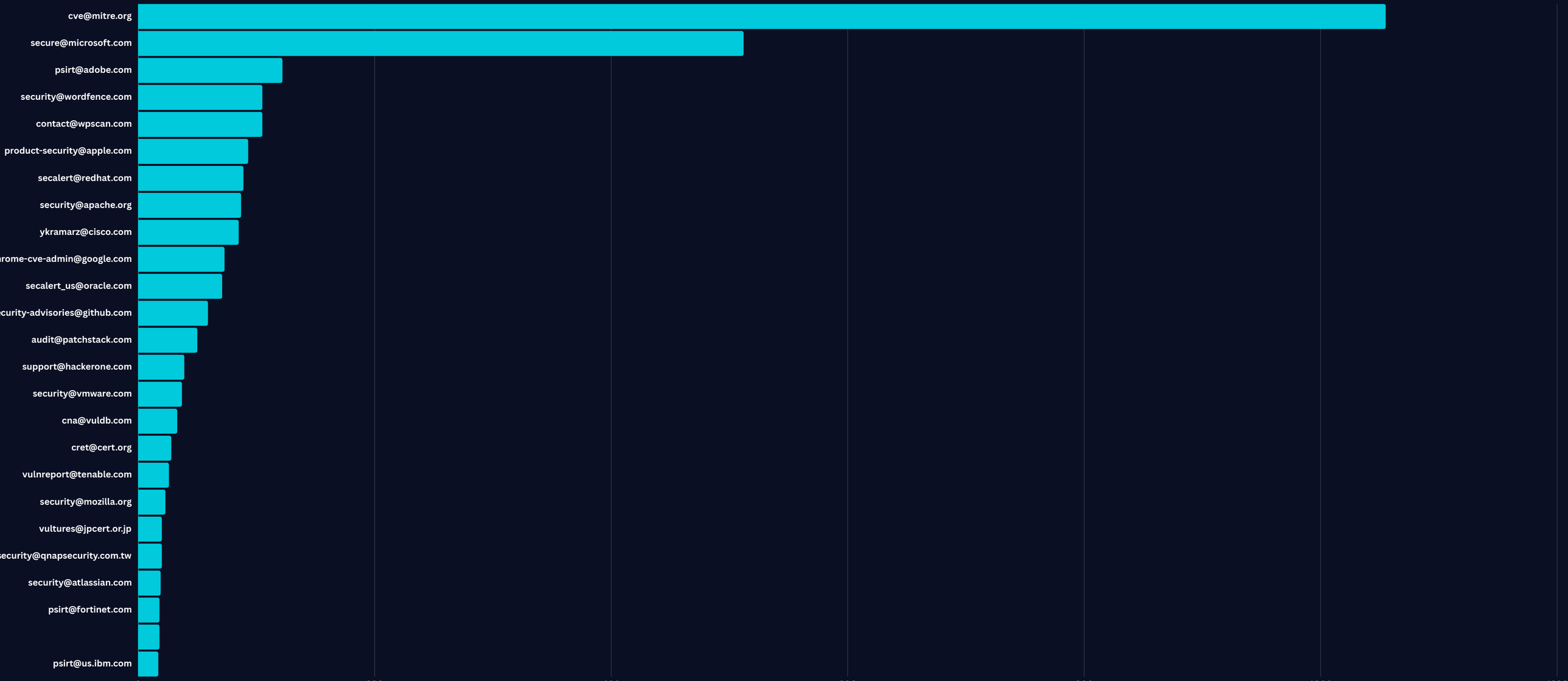


VulnCheck

What CNA’s are associated with the most KEVs?

Top 25 CNA’s for KEV by Unique CVE’s

Source: VulnCheck KEV



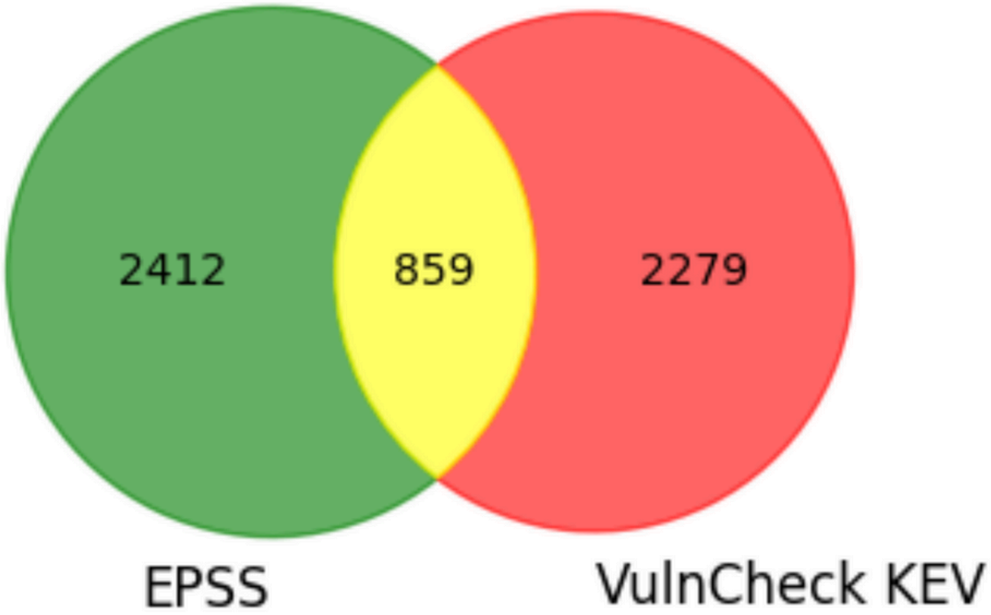
Year CVE Published

VulnCheck

How Does KEV Compare with EPSS?

KEV and EPSS?

EPSS and VulnCheck KEV Interactive Venn Diagram



EPSS Threshold

0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.88

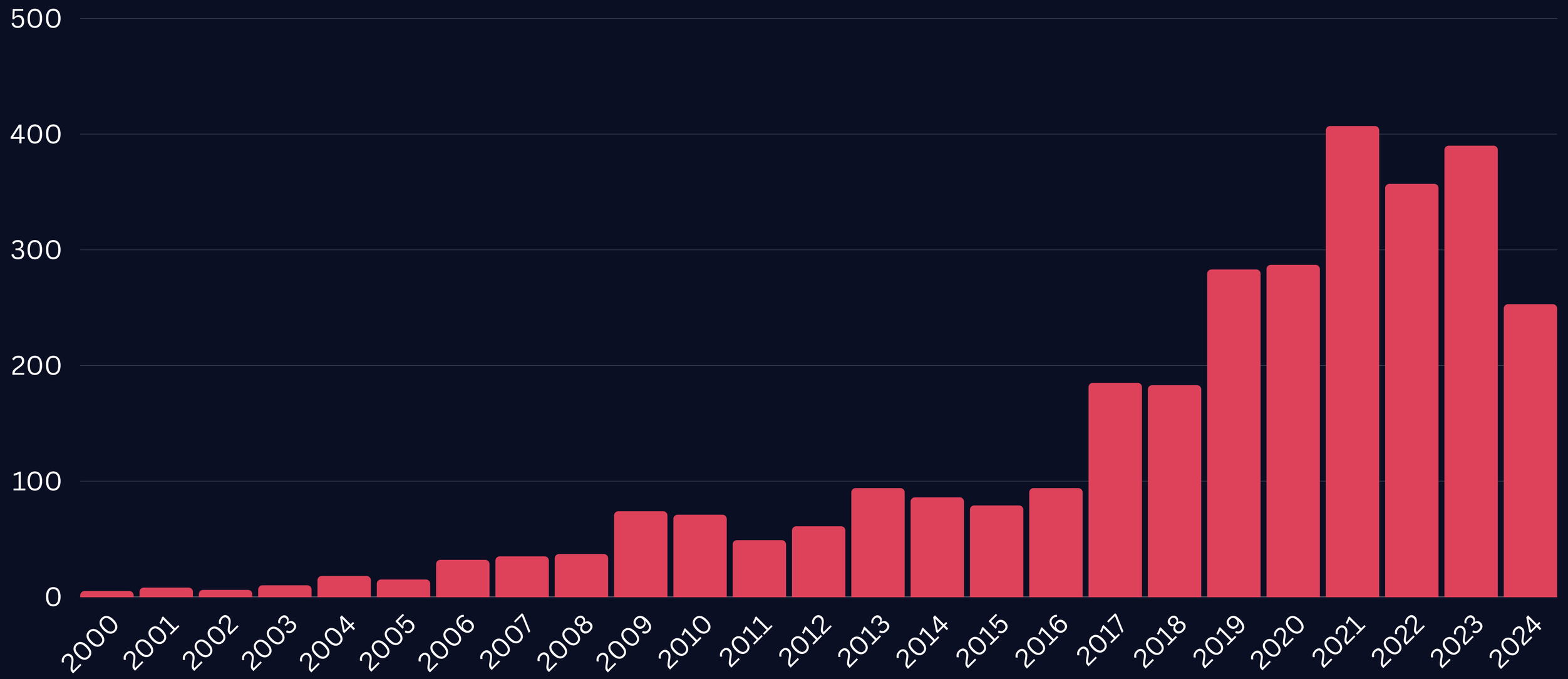
Selected EPSS Threshold: 0.88

Category	Count
Only EPSS	2412
Only VulnCheck KEV	2279
Both	859

Why are KEV and High EPSS Scores so Different?

VulnCheck KEV (CVE Publish Date)

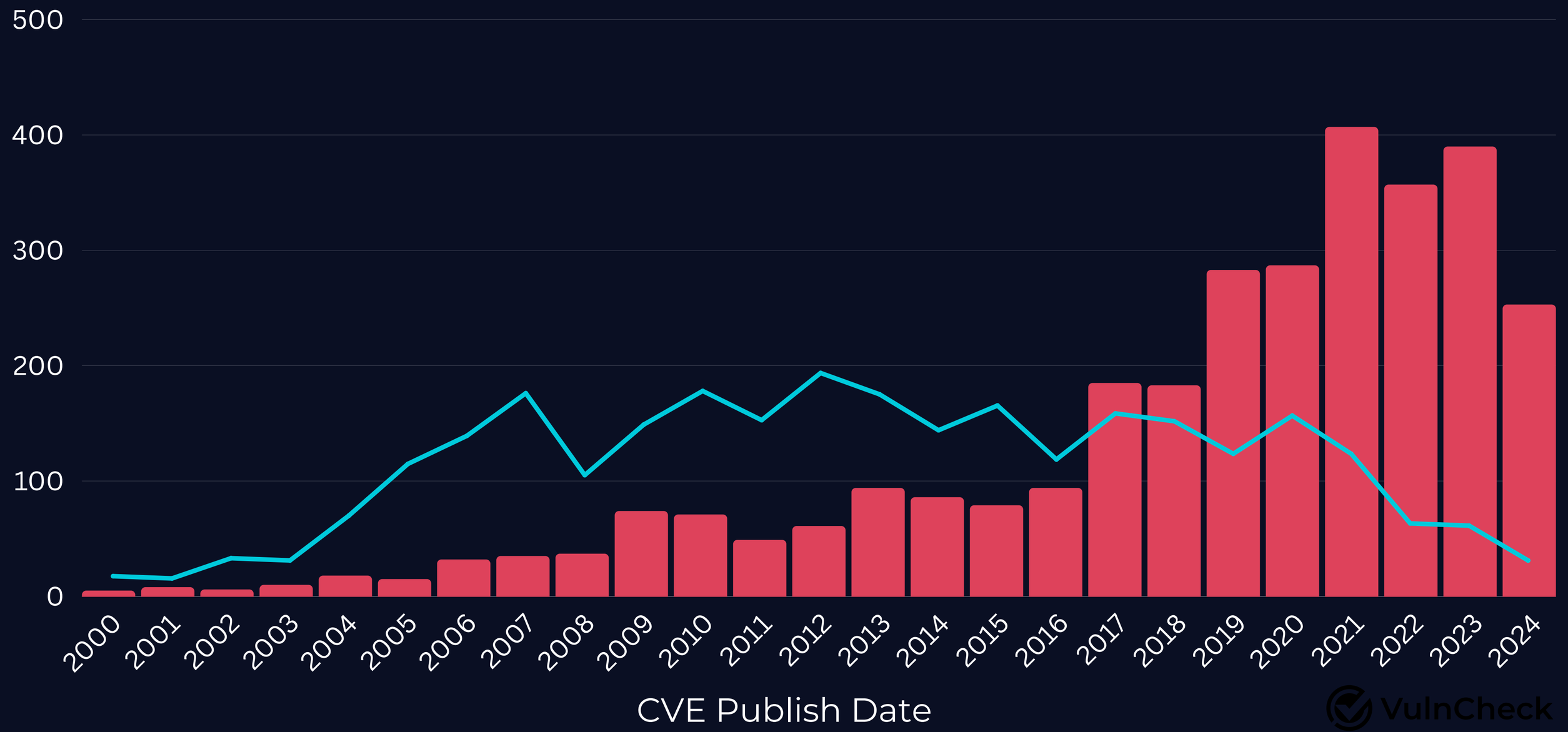
Source: VulnCheck KEV



VulnCheck

VulnCheck KEV w/ EPSS .887

Source: VulnCheck KEV



VulnCheck

Why is the EPSS score so low when there is known exploitation?

VULNCHECK KEV EXPLOITATION TIMELINE

CVE-2020-15415 | DRAYTEK

EPSS Scores

0.02

2023-02-15

Exploitation Confirmed

Source: Palo Alto Networks
Mirai Variant V3G4 Targets IoT Devices
Added to VulnCheck KEV

0.022

2024-02-01

Exploitation Activity First Seen*

Source: ShadowServer

0.017

2024-09-18

PRC Botnet Report

Source: Five Eyes

0.017

2024-09-30

Exploitation Confirmed

Source: CISA

.943

2024-10-01

VULNCHECK KEV EXPLOITATION TIMELINE

CVE-2020-15415 | DRAYTEK

EPSS Scores

0.02
2023-02-15

0.022
2024-02-01

0.017
2024-09-18

0.017
2024-09-30

.943
2024-10-01

Added to VulnCheck KEV

Source: Palo Alto Networks
Mirai Variant V3G4 Targets IoT Devices
Added to VulnCheck KEV

Exploitation Activity

Source: ShadowServer

PRC Botnet Report

Source: Five Eyes

CISA Exploitation Confirmed

Source: CISA
Added to CISA KEV

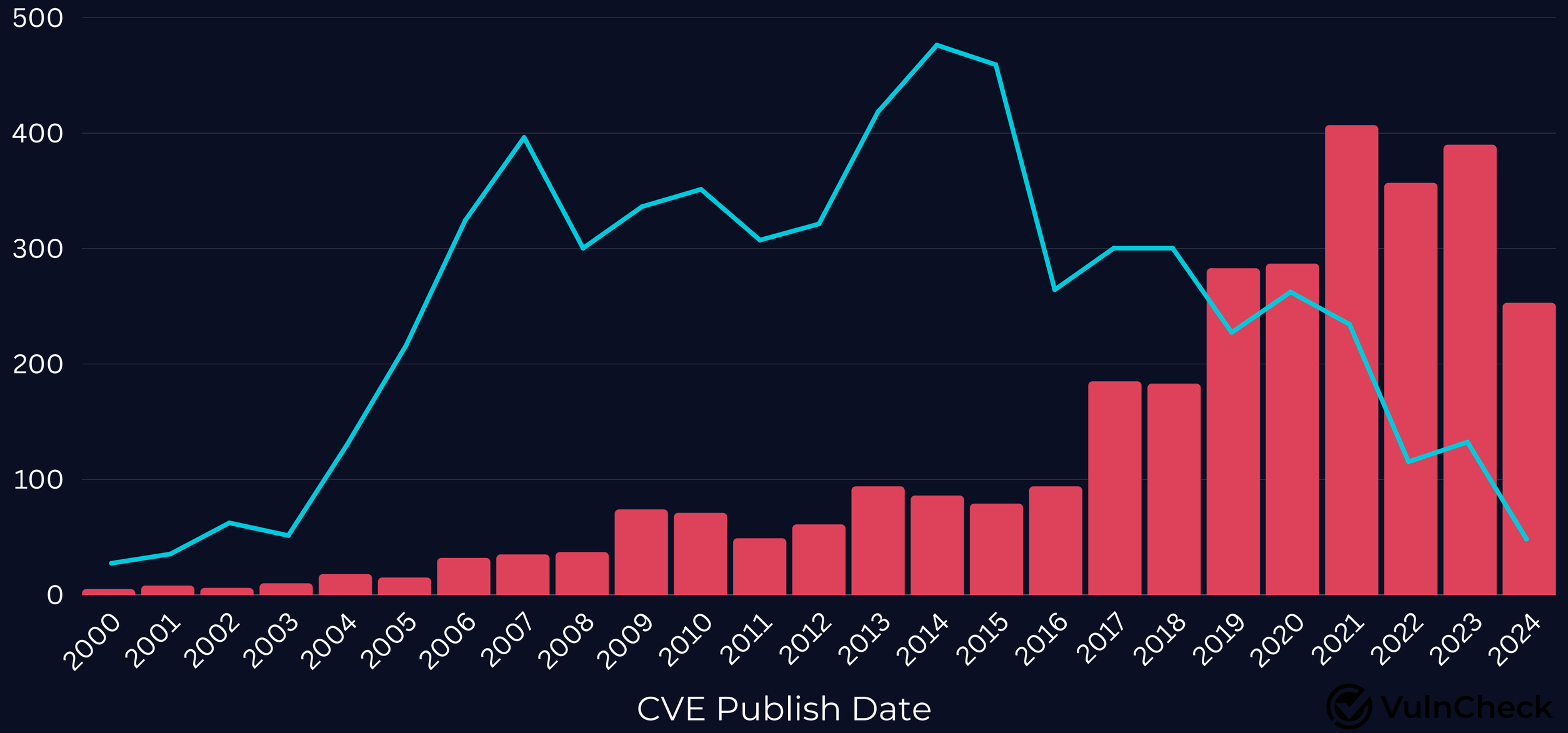
How Might We improve Prediction?

- Increase Access to Exploitation Sources
- Publish Inputs / Outputs from model for a CVE
- More Diverse Exploitation Data Sources
- Opportunity to Catch Early Indicators (Emerging Threats)
- Provide Evidence That Ties Back to why?

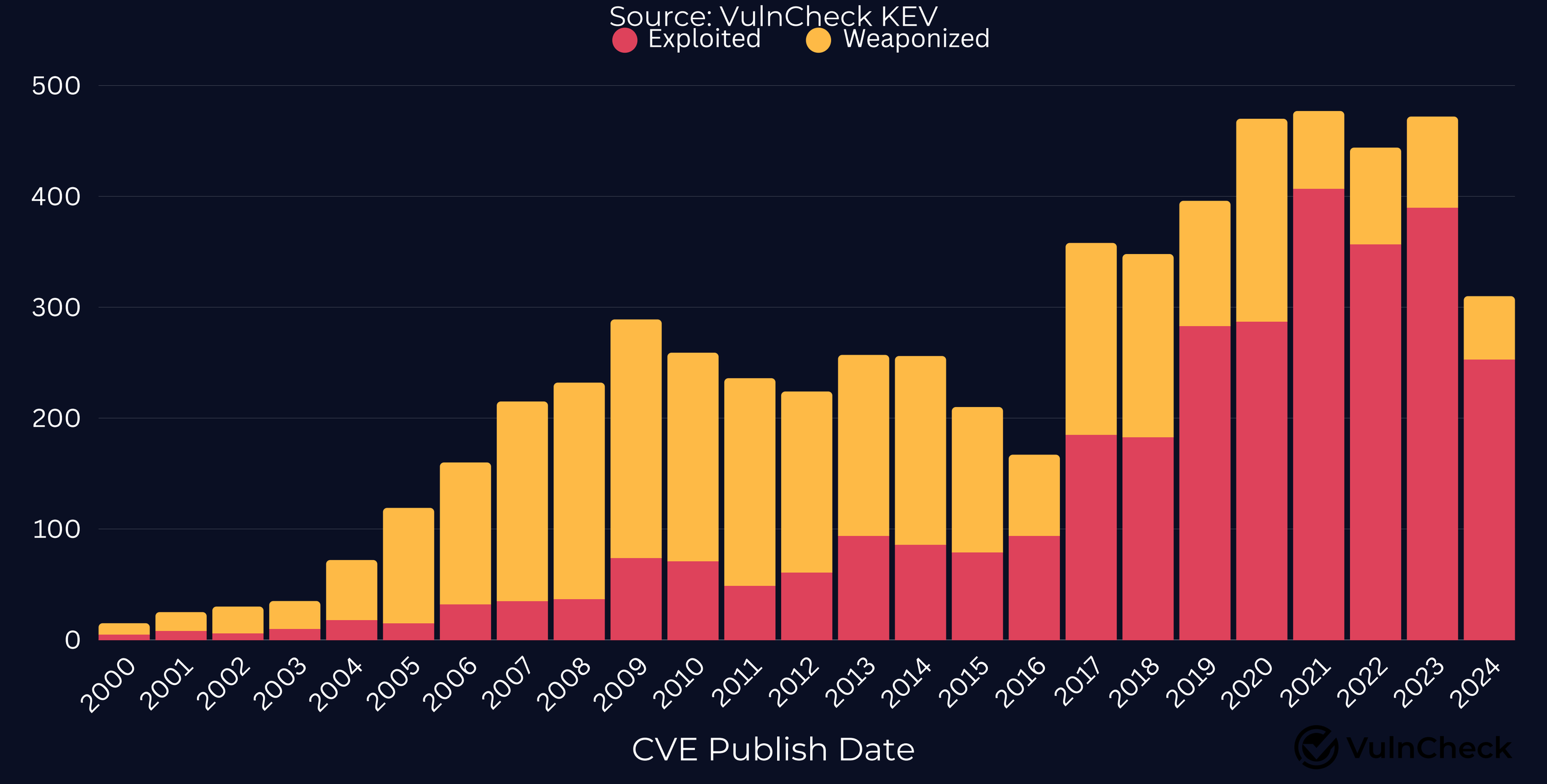
Appendix

VulnCheck KEV+Weaponized w/ EPSS 0.54

Source: VulnCheck EVI / EPSS

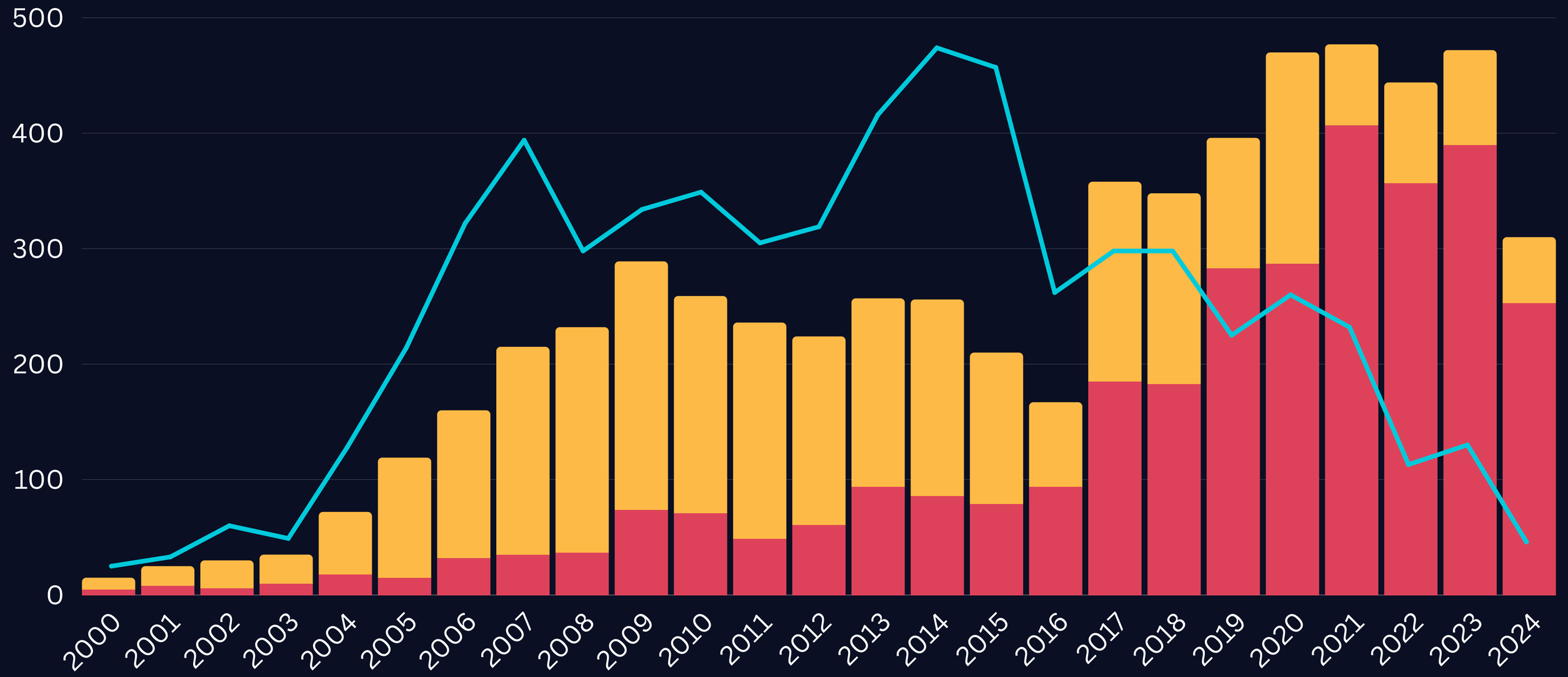


VulnCheck KEV + Weaponized (CVE Publish Date)



VulnCheck KEV+Weaponized w/ EPSS 0.54

Source: VulnCheck EVI / EPSS



VulnCheck

Emerging Threat vs. Vulnerability Debt

Emerging Threat

25%

OF KNOWN EXPLOITED VULNERABILITIES
<=0 Days

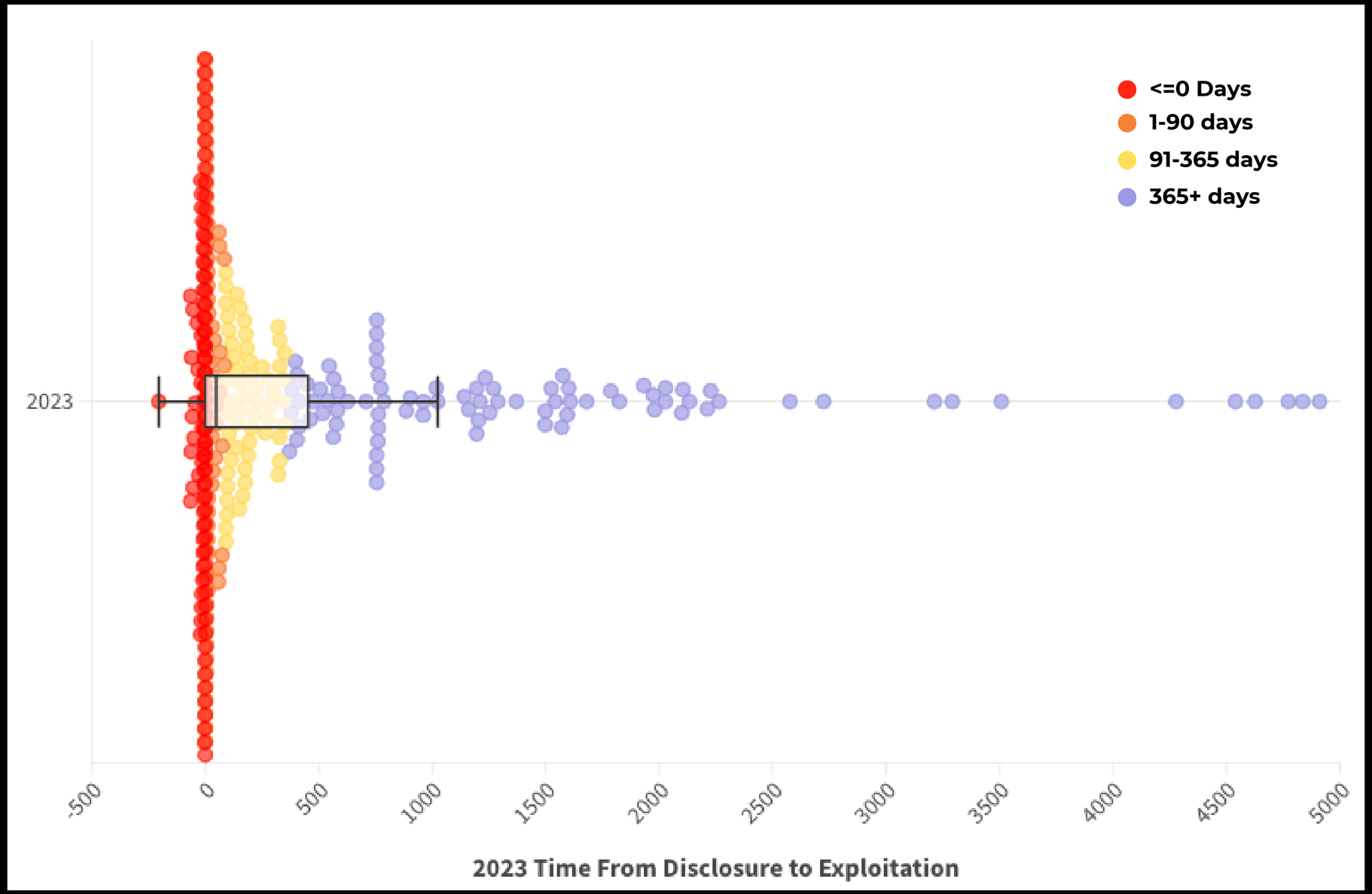
Vulnerability Debt

75%

OF KNOWN EXPLOITED VULNERABILITIES
>=1 Days

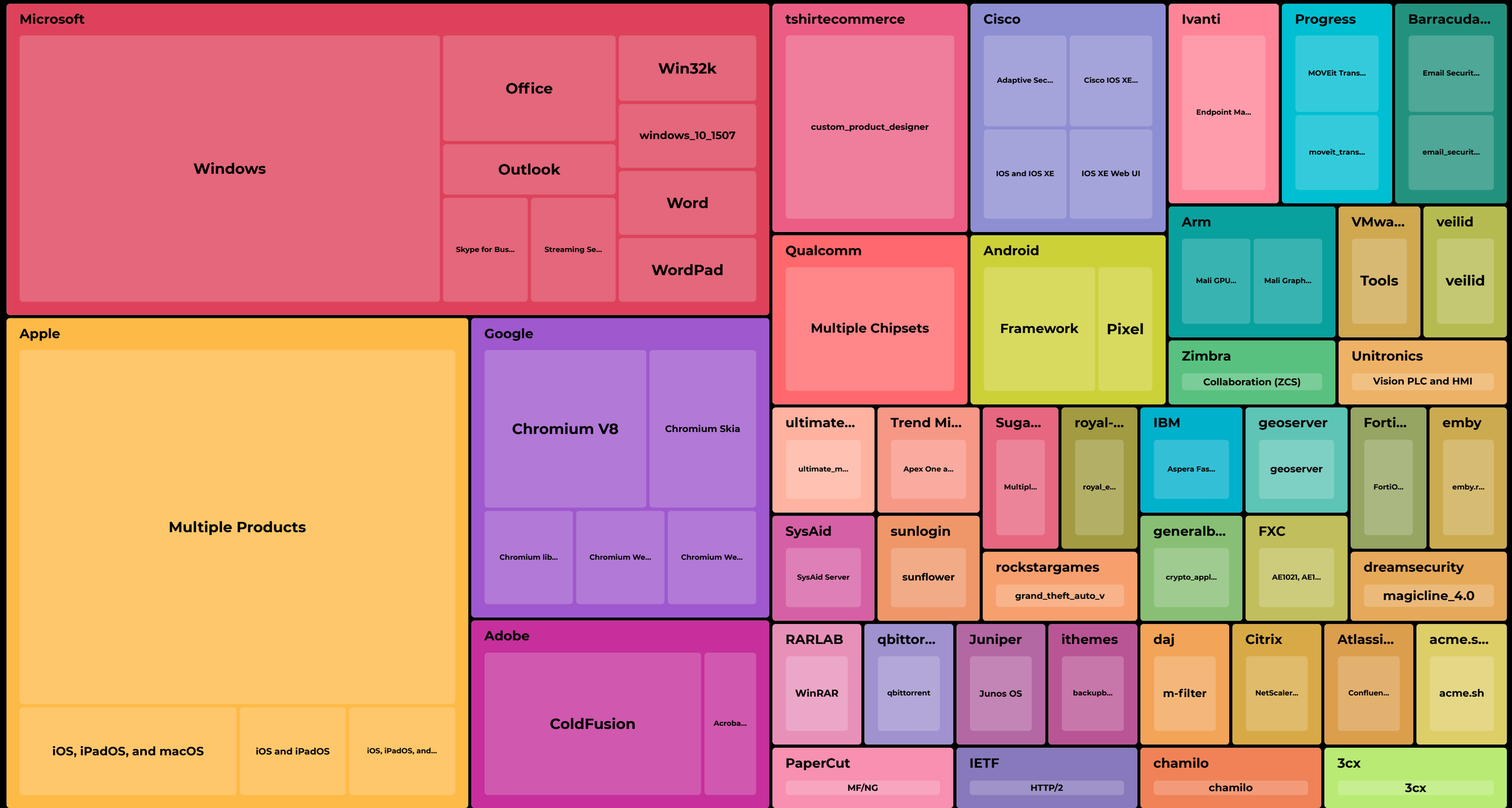
Exploitation Evidence <=0 Days

2023 Time From CVE Disclosure to Exploitation Disclosure



Source: VulnCheck

2023 Vulnerabilities w/ Exploitation Evidence at Time of Disclosure (<=30-days)



Emerging Threat

1. **Rapid Response**
2. **Internet Facing**
3. **End User Interaction**
4. **Remotely Exploitable**

Vulnerability Debt

1. **Root Cause Analysis**
2. **Improve Patch Management**
3. **Implement Best Practices**
4. **Prune Unused / EOL**

VulnCheck Enrichments

3,139+ CAPEC Mapping

91,420+ Mitre Att&ck Mapping

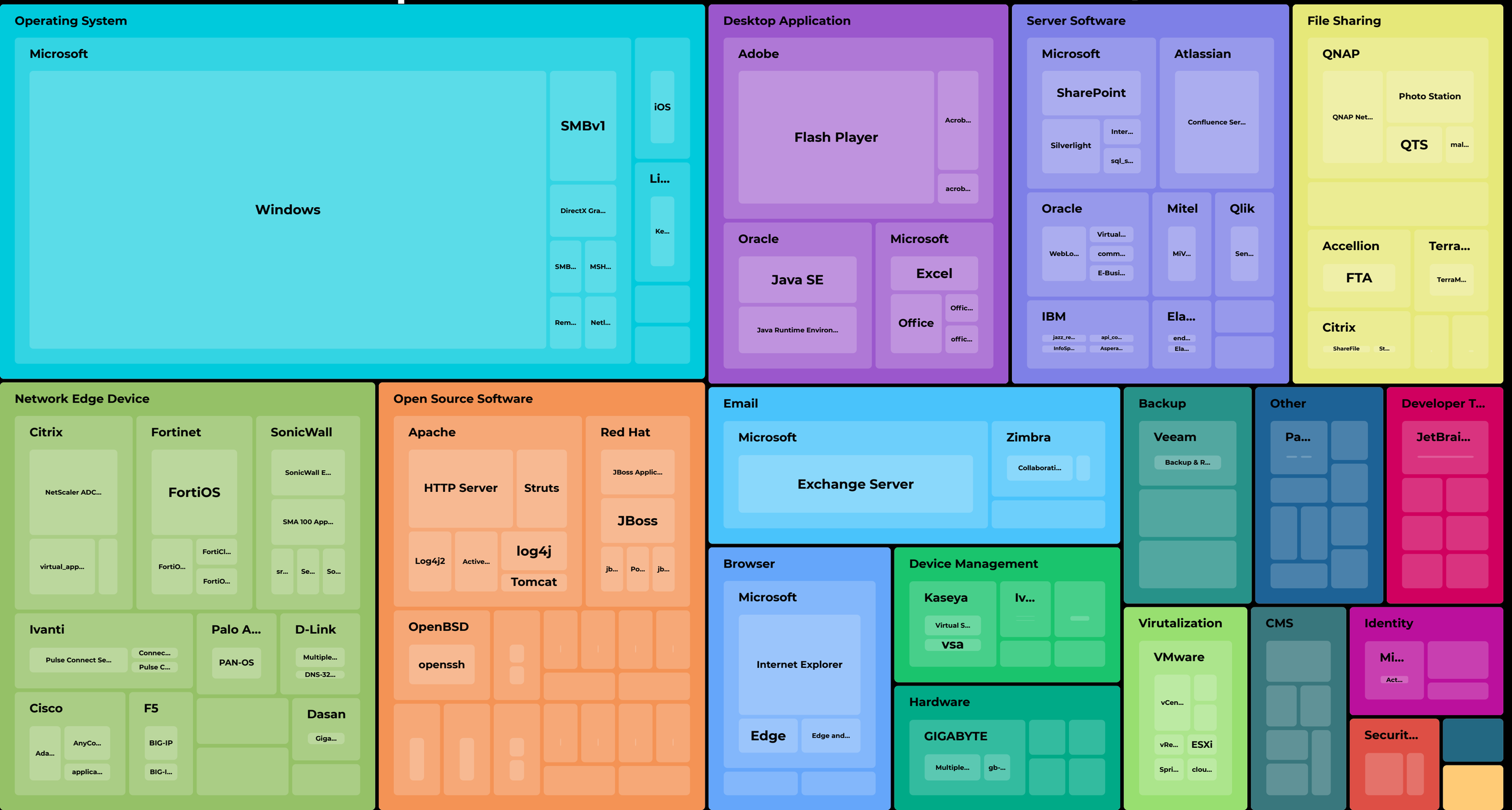
4,588+ Threat Actors

500+ Botnets

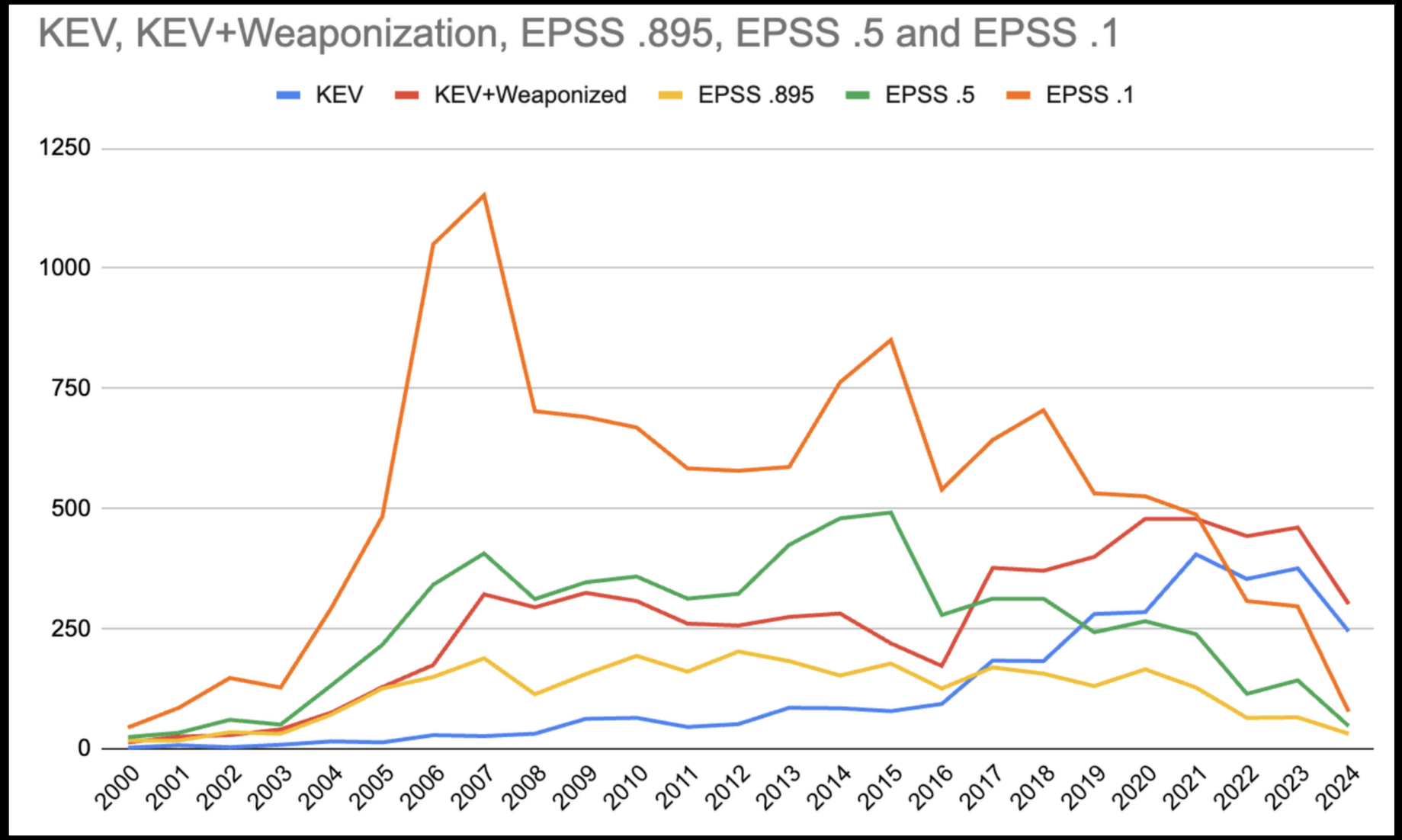
443 Ransomware

443 CPE

2023 Known Exploited Vulnerabilities Associated w/ Ransomware



What’s inside KEV



Focus on Newer Vulnerabilities