Exploited CVEs of 2024: Lessons for Vendors and Defenders

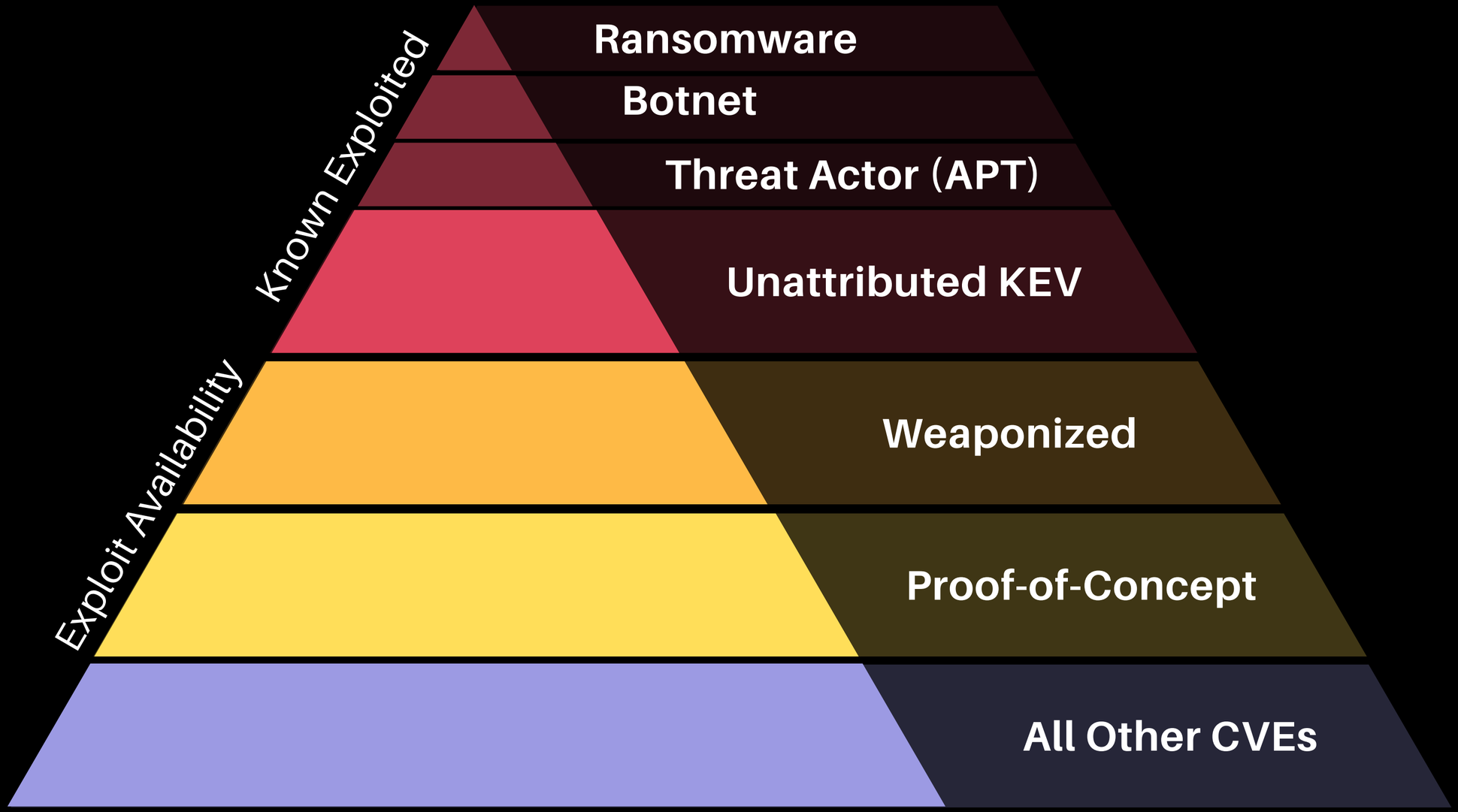
VulnCheck

SECURITY RESEARCH CNA


DON'T
SHOOT THE
MESSENGER

Transparent as Possible About Exploitation

Vulnerability Threat Matrix



VulnCheck

Known Exploited Vulnerabilities

Not Just CISA KEV

How are we defining KEV?

We include any vulnerability publicly-reported as exploited in the wild. It’s Free!

Trusted Sources
Automated KEV

Automated collection &
Third Party Reporting
that is Currated by
security reasearch.

Important Details about KEVs

- Emerging Threat (Fix Fast)
- Evidence is all Public Record
- If there is no CVE > Coordinate to get a CVE issued timely
- Work Closely with other Intel firms on vulnerability / exploitation disclosure
- There are many ways people define exploitation differently

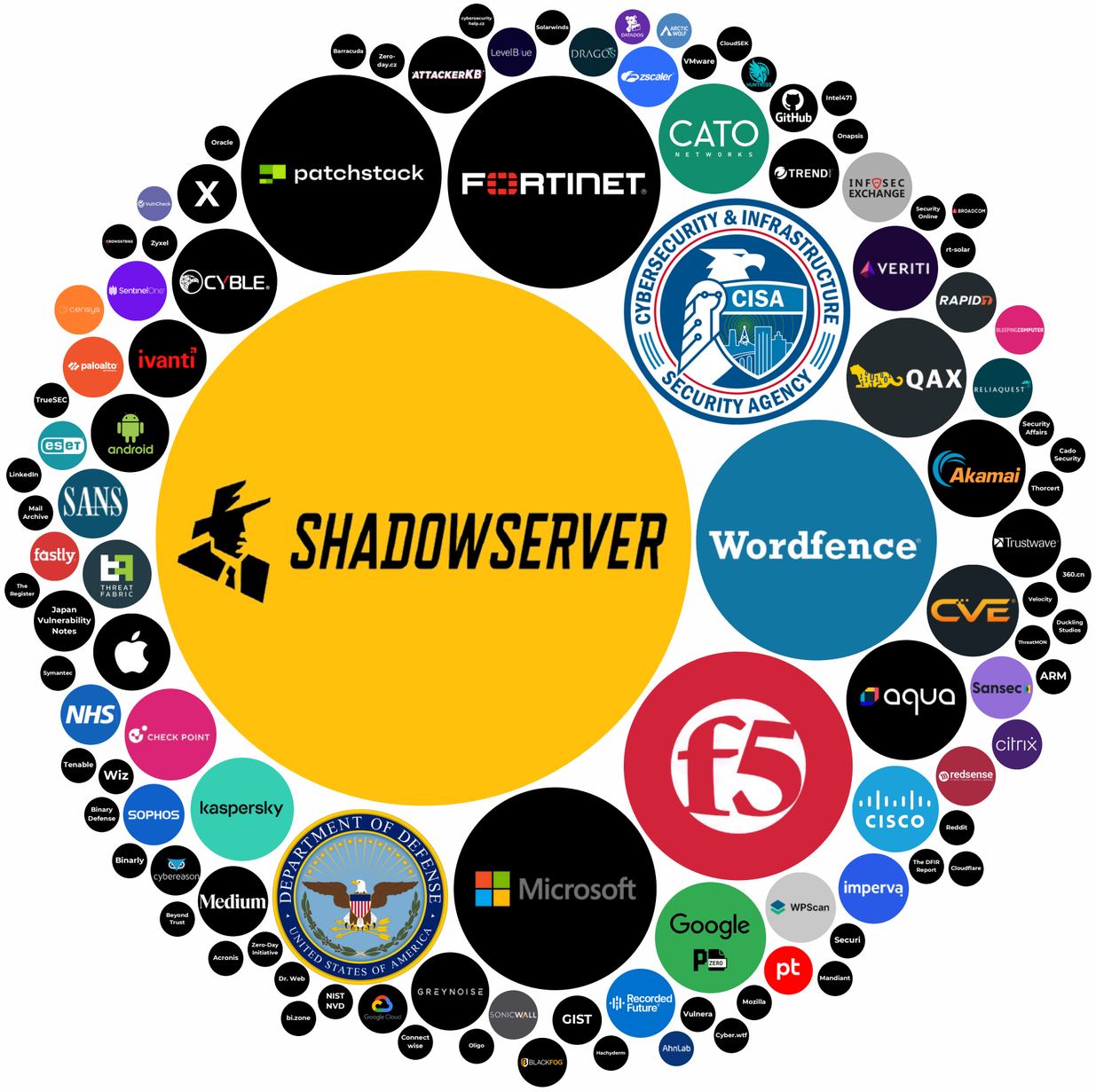
What Does This Research Include?

- Exploitation that was disclosed for the first time in 2024.
- 800+ Known Exploited Vulnerabilities
- 2,000+ KEV Reference Citations*
- 100+ Unique Sources
- 53 Known Ransomware

Dates = When First Evidence was published

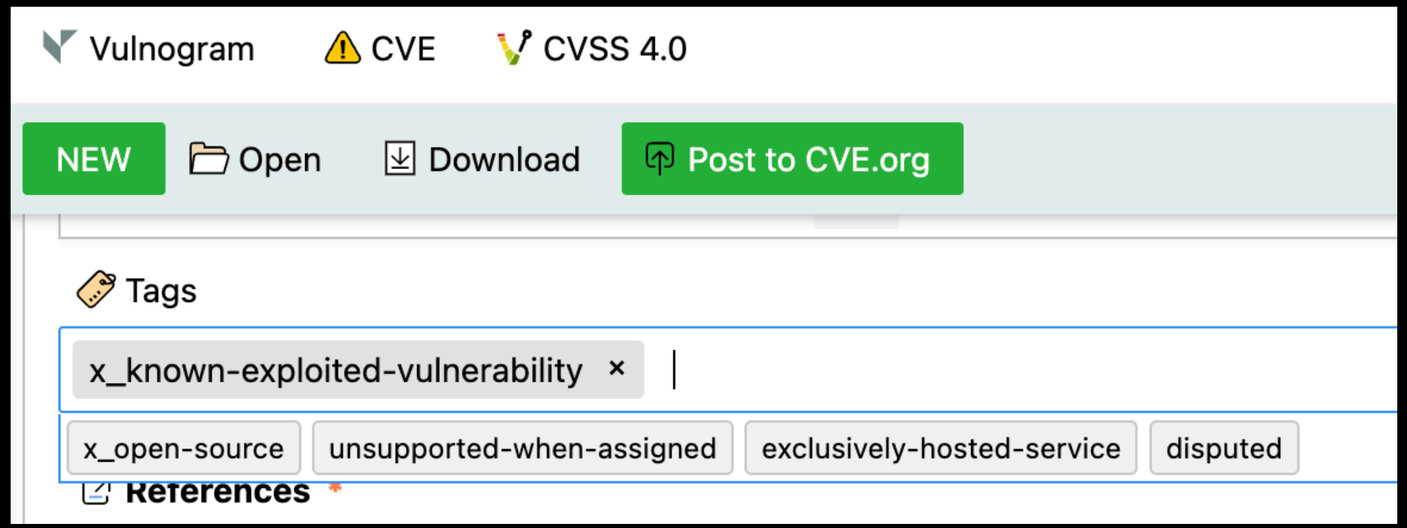
Earliest Reporting Source for Exploitation in the Wild

Source: Vulncheck KEV (2024)



Vendors / CNAS

- Disclose When There is Evidence of Exploitation.
  - Advisories
  - CVE Record
  - Description



Let’s Take a Look at Known Exploited Vulnerabilities Identified in 2024

VULNCHECK KEV EXPLOITATION TIMELINE

CVE-2023-22527 | ATLASSIAN CONFLUENCE SERVER

01/21

Exploitation Confirmed

Source: @TheDFIRReport

Added to VulnCheck KEV

1 VulnCheck XDB Exploit Link Available (1/17)

01/22

Exploitation Confirmed

Source: ShadowServer

01/22

3 Exploits Available

Source: Github

3 VulnCheck XDB Links Provided

1/22

Exploitation Confirmed

Source: SANS Internet Storm Center

1/23

Exploitation Confirmed

Source: @catc0n Vulnerability Research Director @Rapid7

1/23

Exploitation Confirmed

Source: Tenable Research Advisory

1/23

3 Exploits Available

Source: Github

3 VulnCheck XDB Links Provided

1/24

Exploitation Confirmed

Source: Added to CISA KEV

1/24

3 Exploits Available

Source: Github

3 VulnCheck XDB Links Provided

2/01

Exploitation Confirmed

Source: Fortiguard Threat Signal Report

2/02

1 Exploit Available

Source: Github

1 VulnCheck XDB Link Provided

2/14

CISA KEV Due Date

Source: CISA KEV

2/21

Exploitation Confirmed

Source: Imperva Threat Research

VulnCheck

VULNCHECK EXPLOIT TIMELINE

CVE-2024-35250 | Microsoft Windows

	CVE Published by Microsoft Source: CVE.org	1st Exploit Available Source: Github	2nd Exploit Available Source: Github	Weaponized Exploit Source: Metasploit	4th Exploit Available Source: Github	5th Exploit Available Source: Github	Exploitation Evidence Source: CISA KEV
EPSS Score	0.00043	0.00043	0.00043	0.00043	0.00043	0.00043	0.00043

CVSSV3.1 Temporal Score

7.8 High (CNA: Microsoft)

V4 EPSS Score

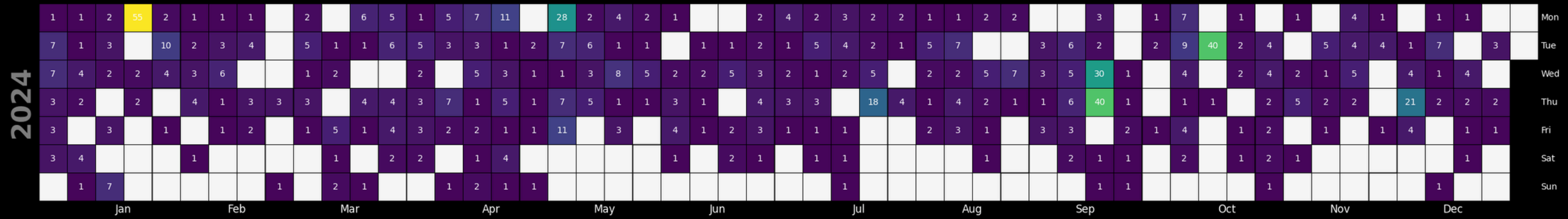
0.85309

March 17th, 2025

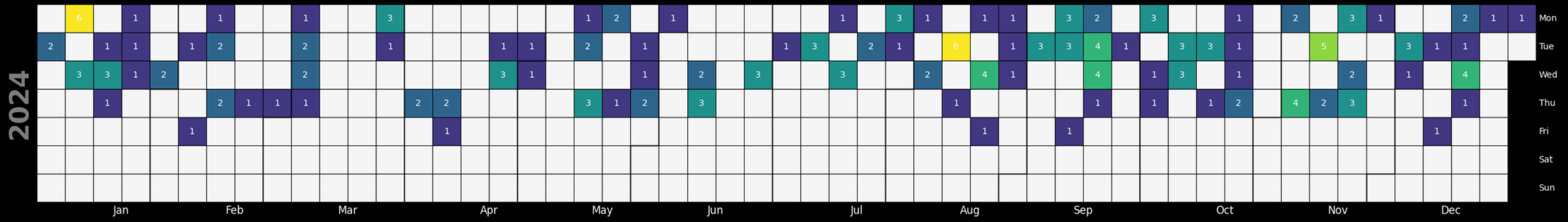
VulnCheck

What Can we Learn about volume / frequency

Known Exploited Vulnerabilities

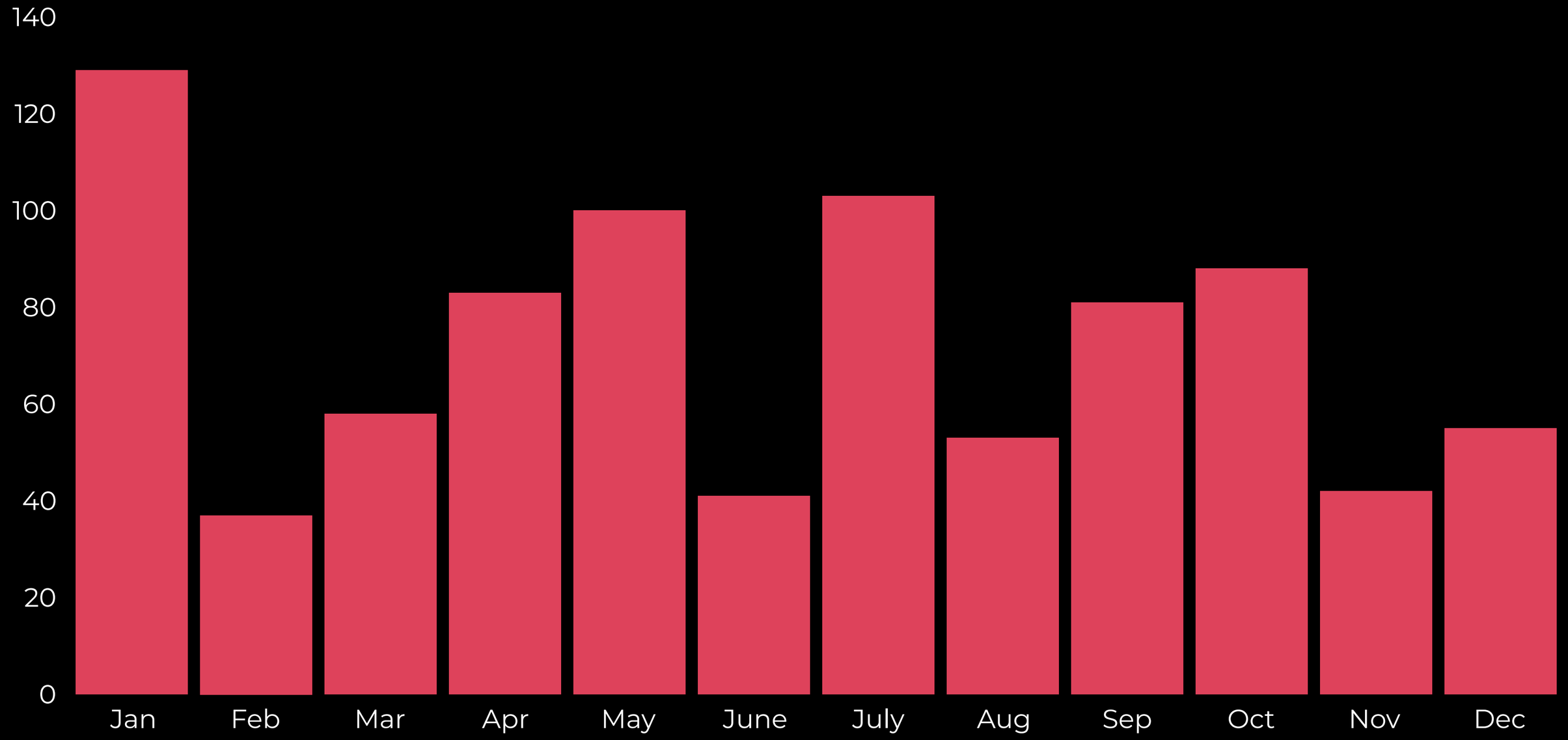


CISA KEV



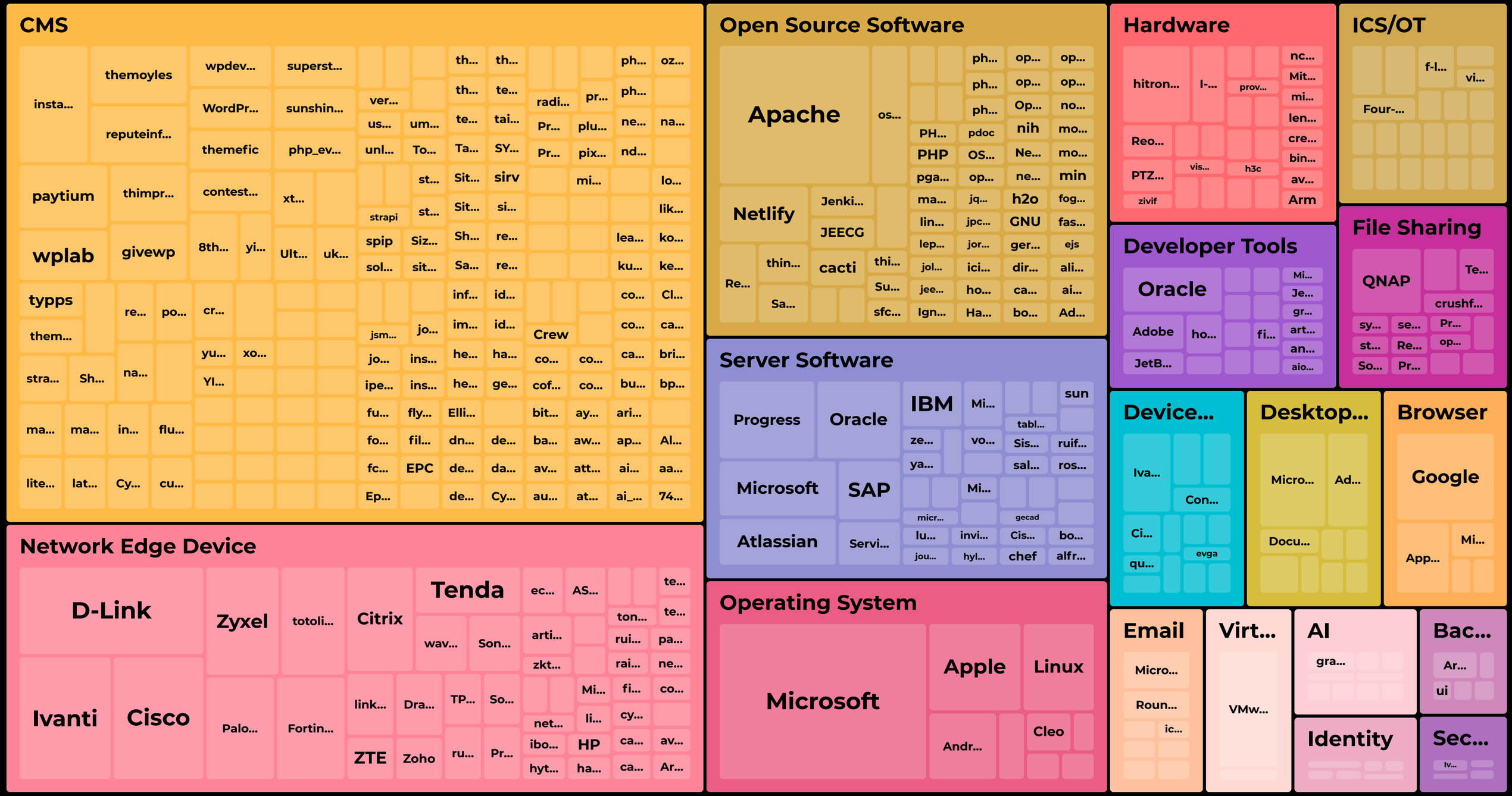
Source: VulnCheck

KNOWN EXPLOITED VULNERABILITIES (2024)



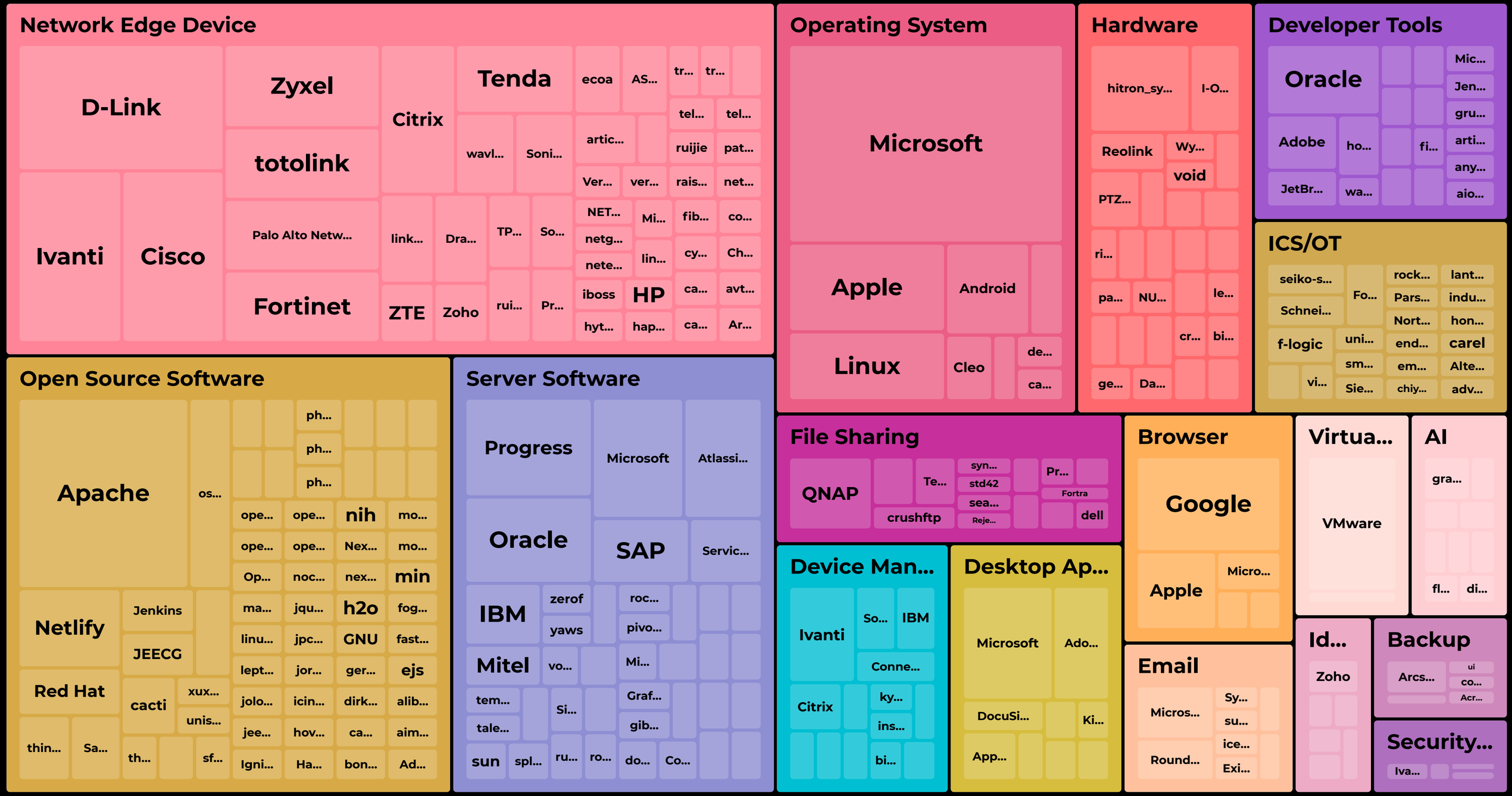
What Categories of Technologies Have Known Exploited Vulnerabilities?

What Types of Technologies Have Known Exploited Vulnerabilties (2024)



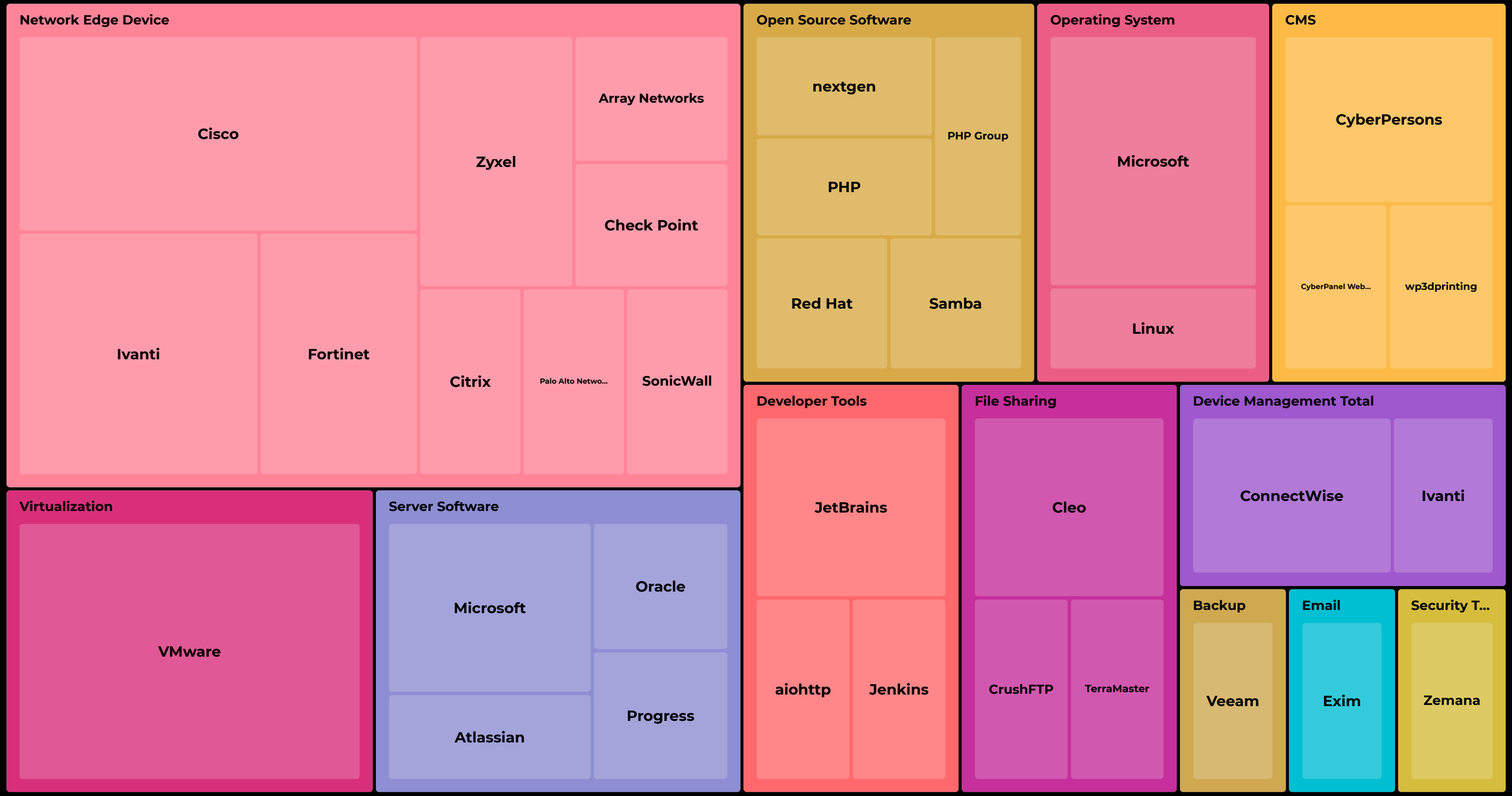
What About Without CMS?

What Types of Technologies Have Known Exploited Vulnerabilties (2024)



Ransomware

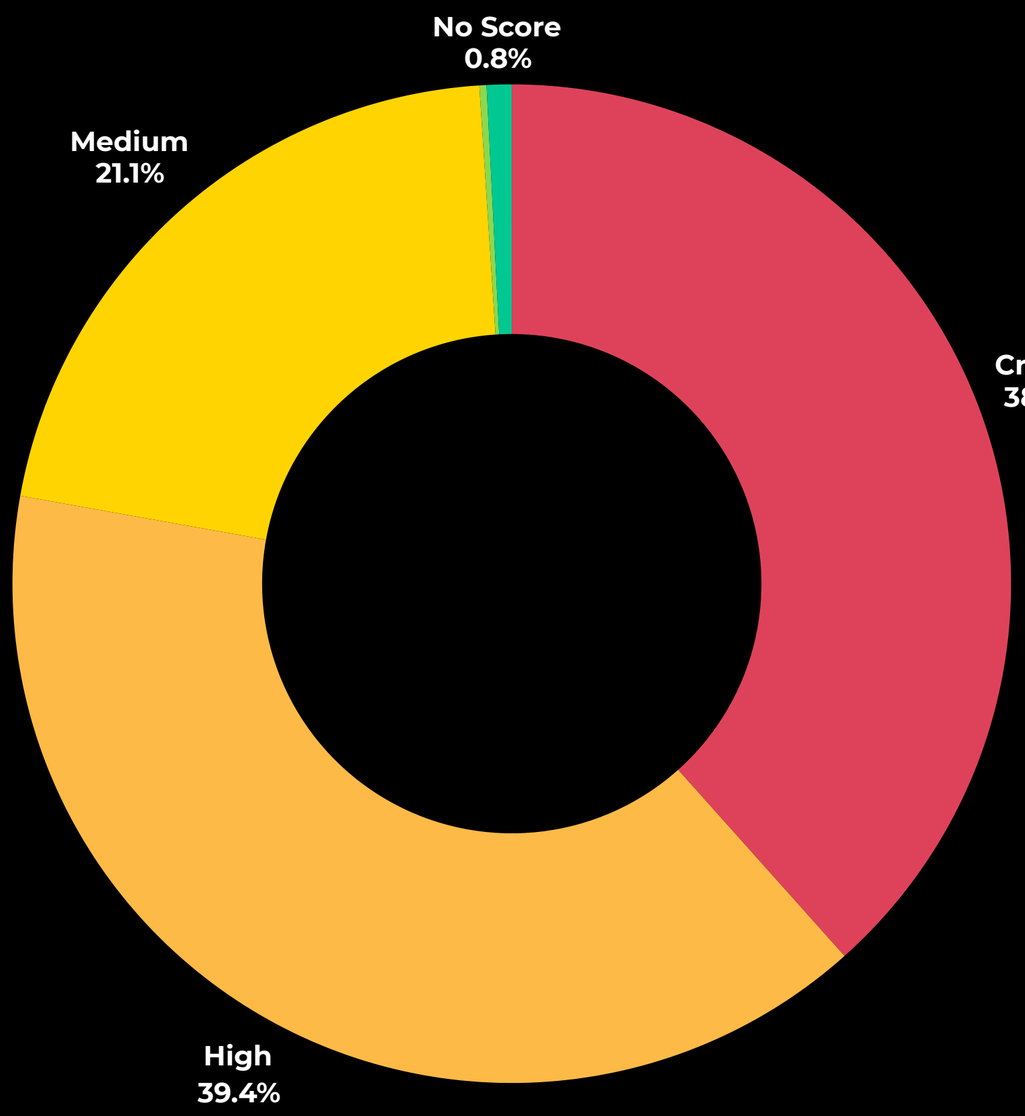
2024 KEVs Associated w/ Ransomware Campaigns



Vulnerability Scoring Systems

What is the CVSS Severity of Known Exploited Vulnerabilities?

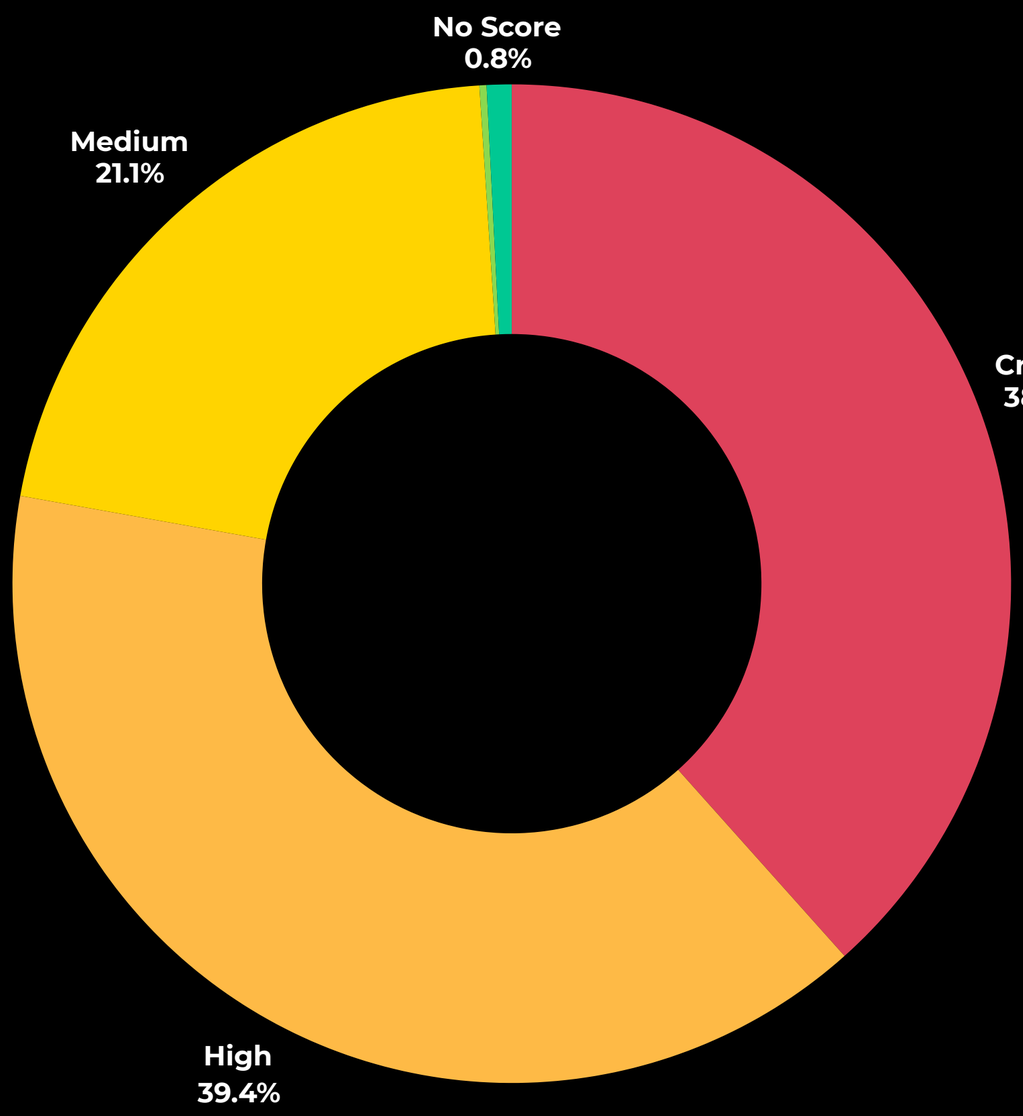
CVSS-B Severity



VulnCheck

Just Use CVSS-BT

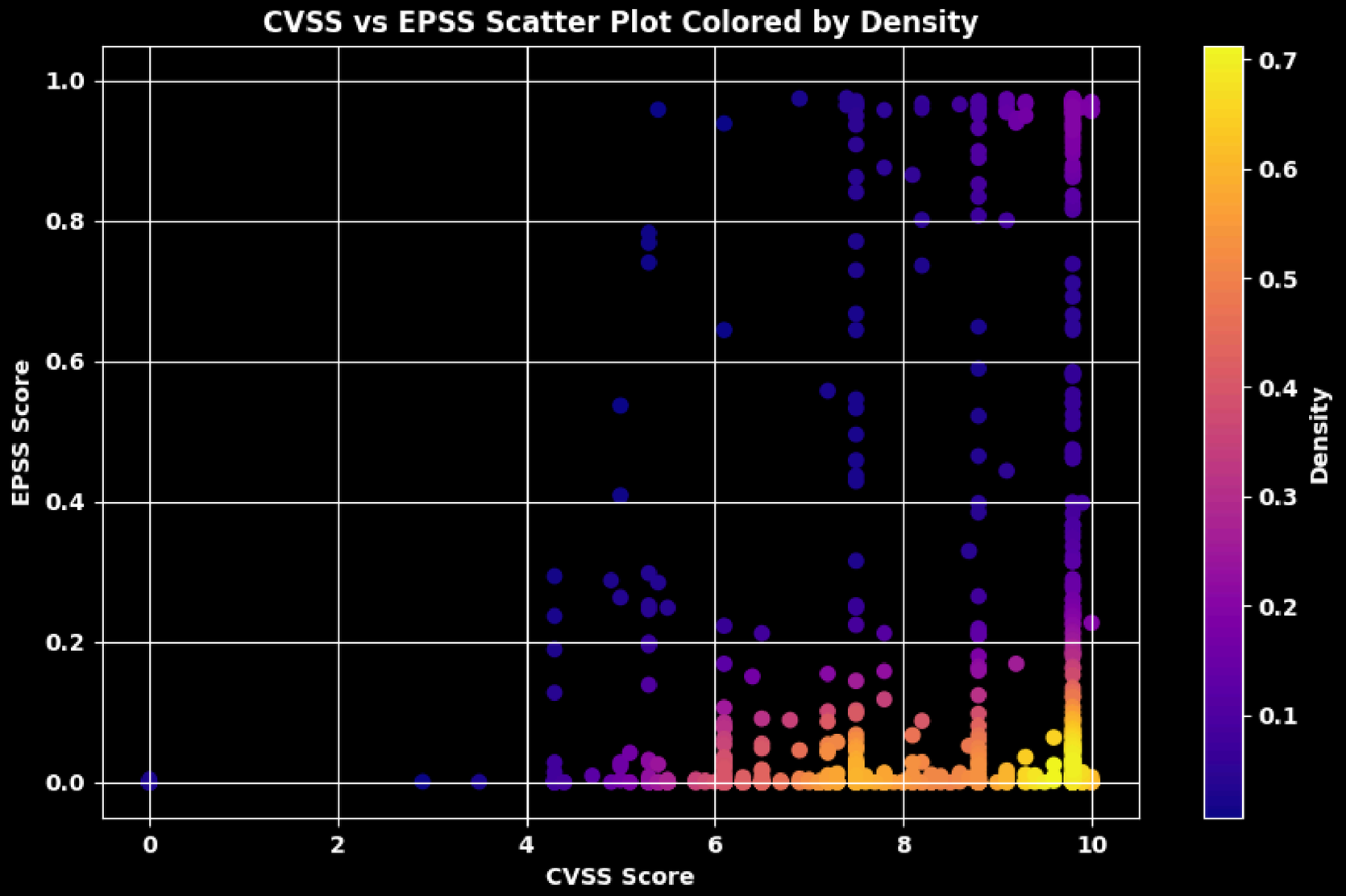
CVSS-BT Severity



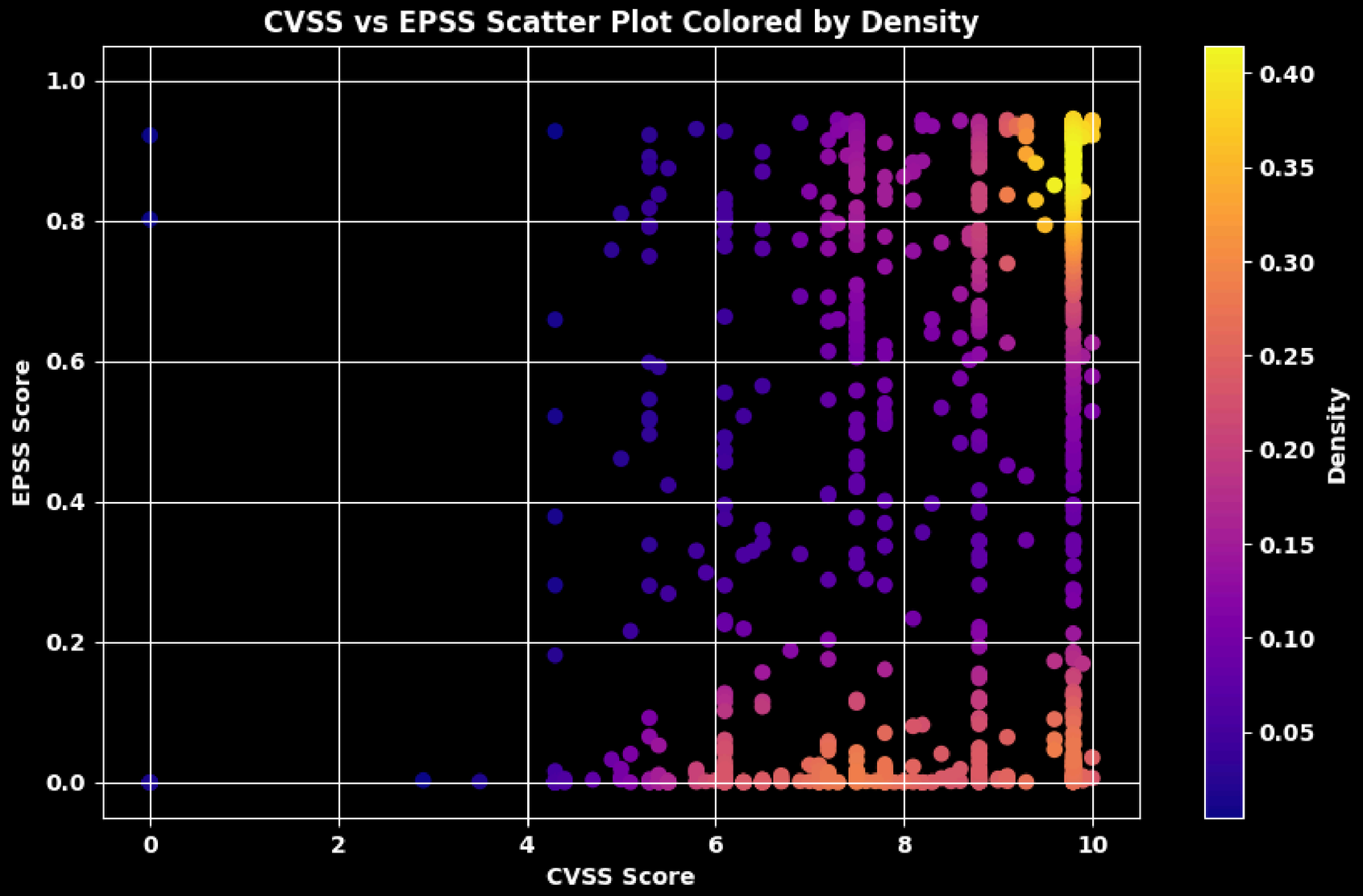
VulnCheck

Did EPSS scoring improve with V4 for 2024 KEVs?

2024 KEVs Mapped to CVSS / EPSS V3



2024 KEVs Mapped to CVSS / EPSS V4



Defender Considerations For Emerging Threat

1. **As a Consumer, become knowledgable in the limitations of scoring systems and cautious on becoming overly dependent on sources that you are not continually monitoring and analyzing and intimately understand how and if they are working.**
2. **Act on available evidence of exploitation, weaponization and other exploit evidence with a sense of urgency.**
3. **Decision Tree Frameworks including SSVC / Risk Based Prioritization (Chris Madden) provides a foundation framework for prioritizing vulnerabilities using broader context.**

Other Considerations for Defenders

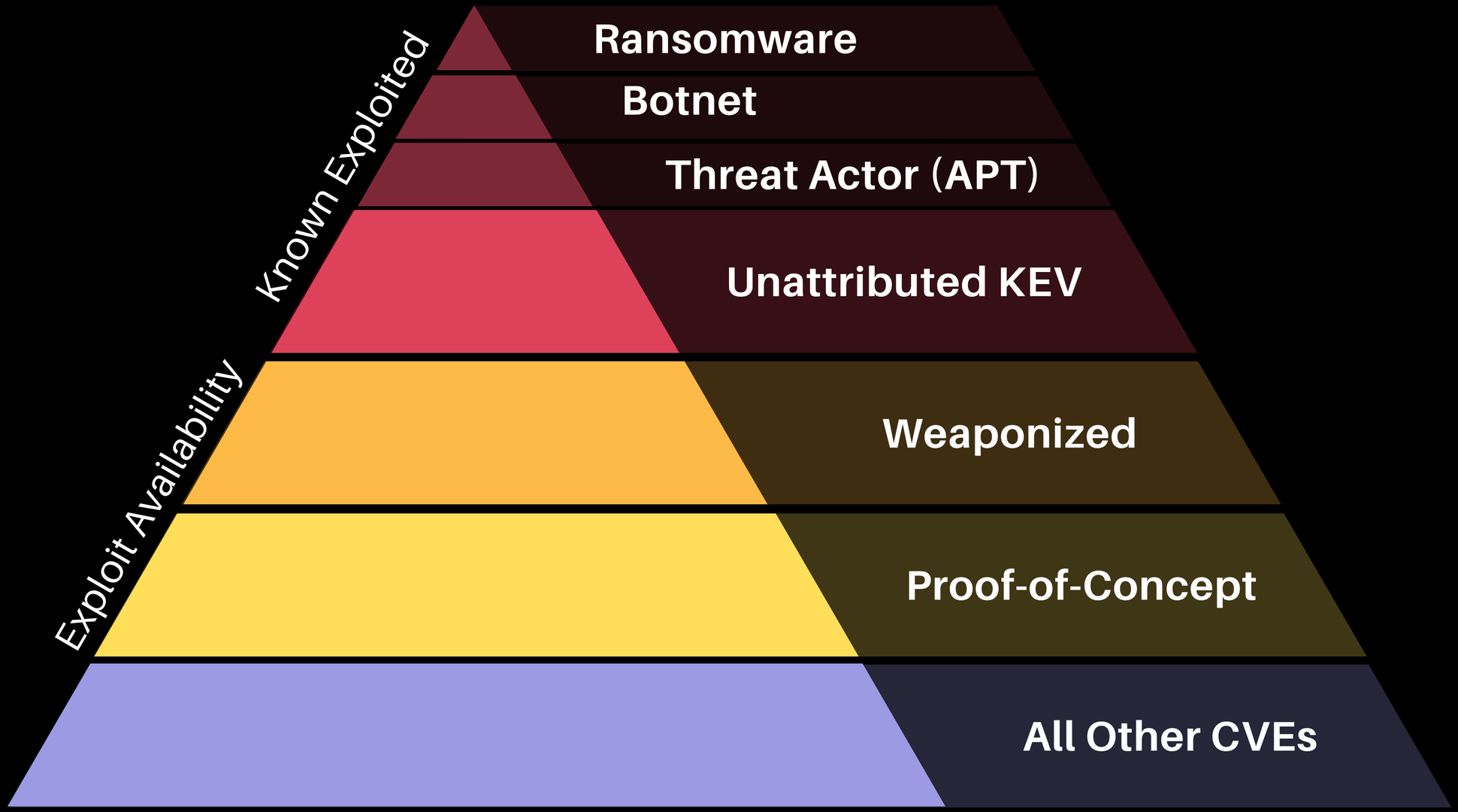
Emerging Threat

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**
5. **Mitagating Controls**

Vulnerability Threat Matrix



VulnCheck

Thank You!