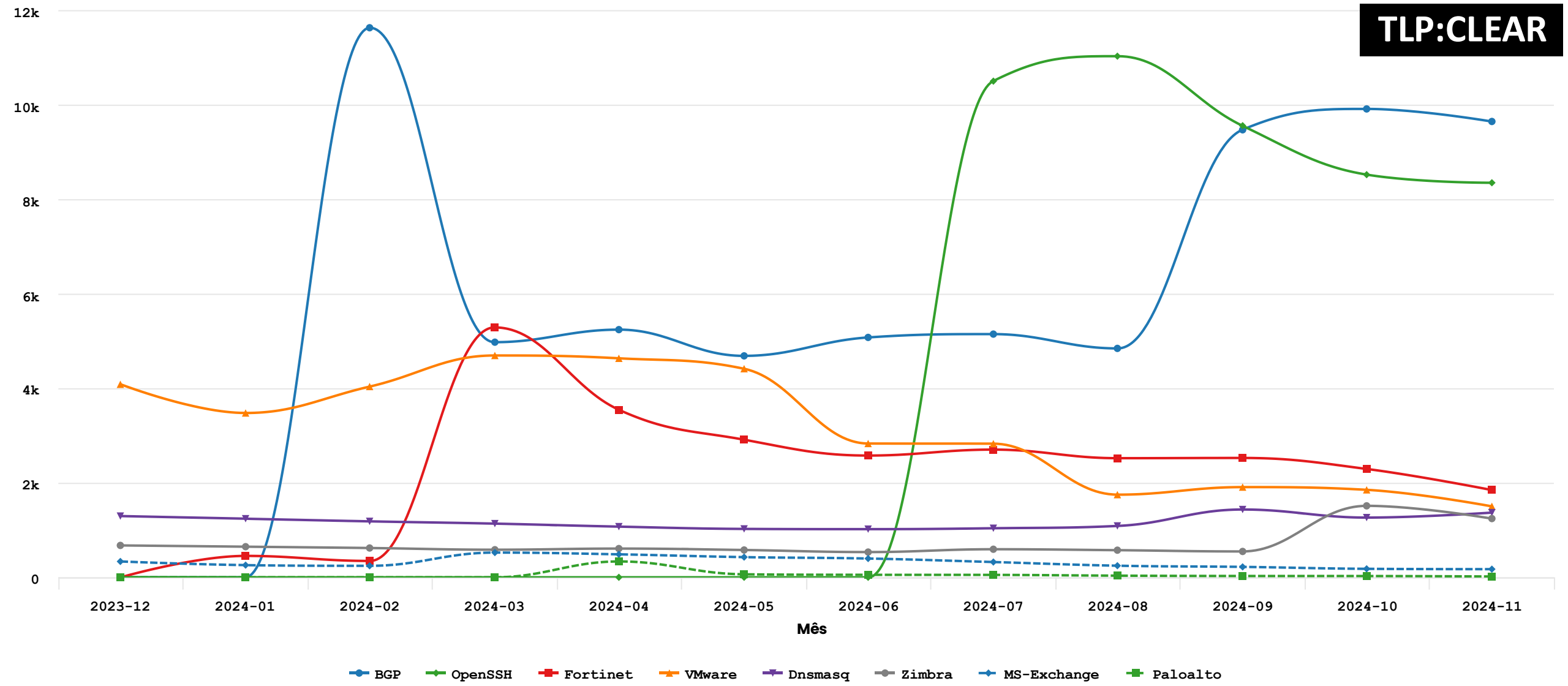
Priorizando Patches: Entendendo CVSS, KEV, EPSS e SSVC

Dra. Cristine Hoepers
Gerente, CERT.br/NIC.br
cristine@cert.br

GTS 39 – 09 de dezembro de 2024
São Paulo – SP

cert.br nic.br cgi.br

TLP:CLEAR



Endereços IP notificados pelo CERT.br
38 CVE + BGP Exposto (RFC 7454 - seção 4)

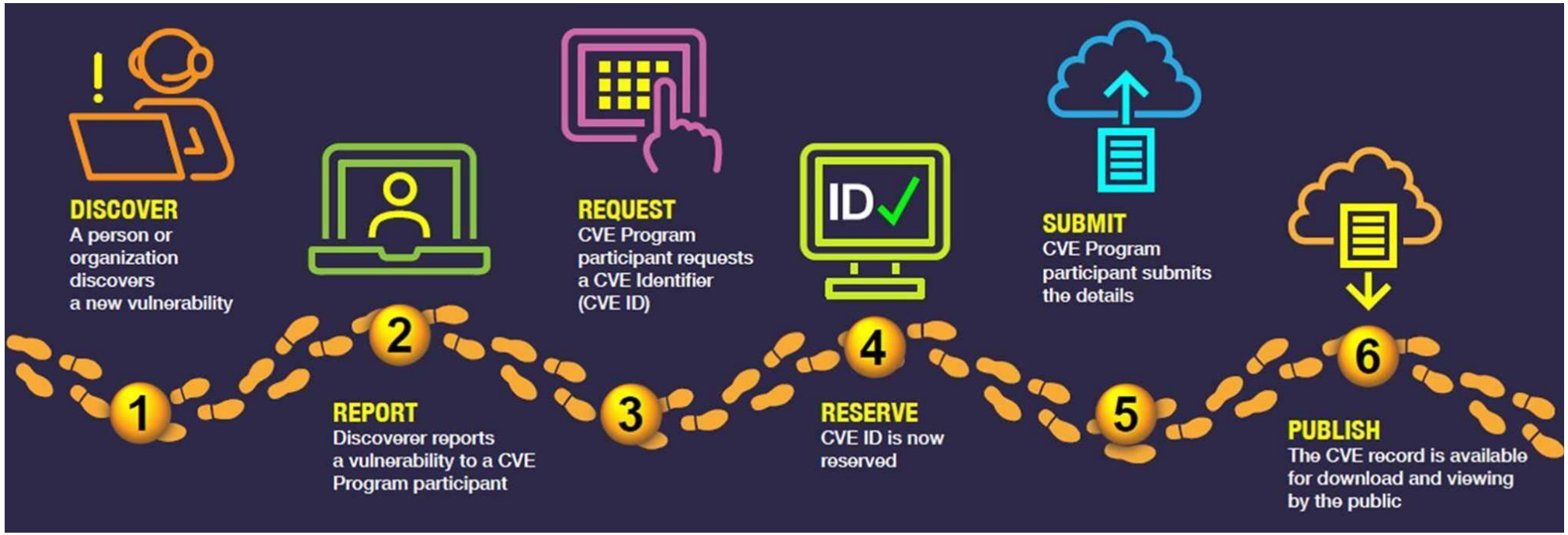
Fonte: https://stats.cert.br/vulns/

CVE – Common Vulnerabilities and Exposures:
“Ou a Vulnerabilidade tem CVE ou não existe”

TLP:CLEAR

“*The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities*.”

“***There is one CVE Record for each vulnerability in the catalog***.”

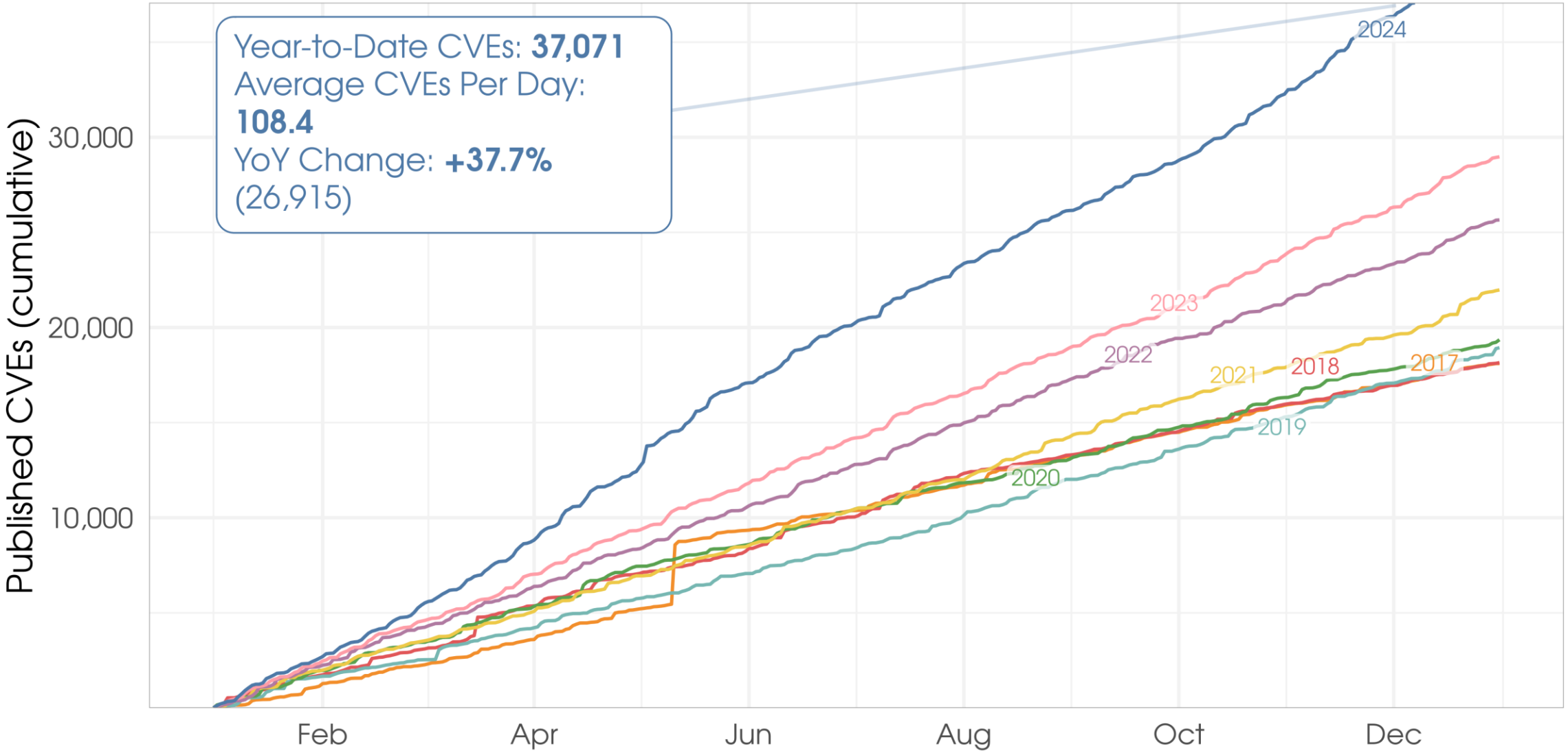


Fonte: https://www.cve.org/About/Process

TLP:CLEAR

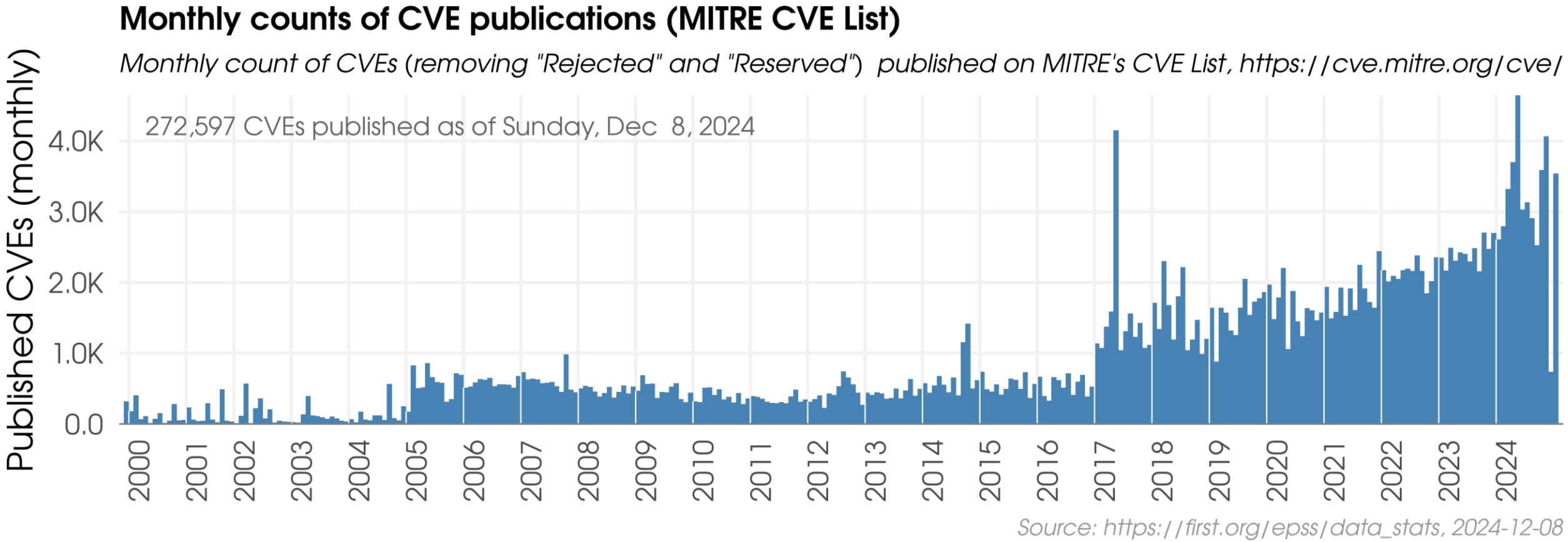
Year-to-date CVE publications (MITRE CVE List)

Lines showing the daily cumulative count of published CVEs on MITRE's CVE List, https://cve.mitre.org/cve/



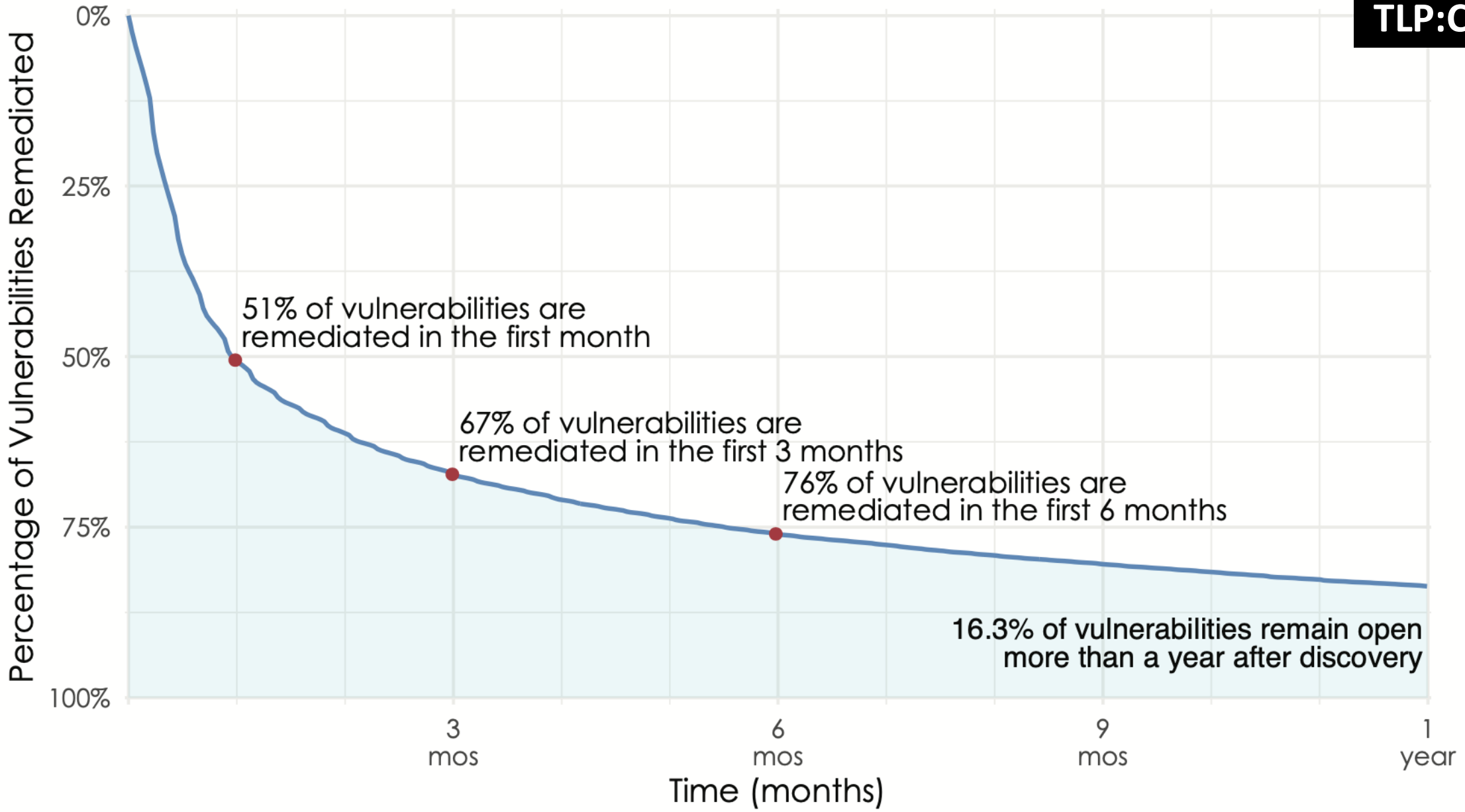
Source: https://first.org/epss/data_stats, 2024-12-08

Fonte: https://www.first.org/epss/data_stats



Fonte: https://www.first.org/epss/data_stats

TLP:CLEAR



Fonte: https://www.cyentia.com/patching-fast-and-slow/ | https://www.cyentia.com/why-your-mttr-is-probably-bogus/

Mais Algumas Estatísticas Globais

- **Mais da metade** das organizações só conseguem **aplicar patches em 15.5%** dos CVEs/mês
  - ¼ corrige menos de 6.6% dos CVEs
- **Menos de 5%** dos CVEs são ativamente **explorados**
- 32% das top 100 vulnerabilidades exploradas na lista do ShadowServer são "*vintage vulnerabilities*"
- CISA KEV (*Known Exploited Vulnerabilities*) tem 46% de "*vintage vulnerabilities*"

Fontes:
https://arxiv.org/pdf/2302.14172
https://www.first.org/resources/papers/vulncon2024/VulnCon-Why-Can-t-We-All-Just-Get-Along.pdf

Gestão de Vulerabilidades

“A prática de identificar, priorizar e corrigir vulnerabilidades de *software* conhecidas.”

Fonte: https://arxiv.org/pdf/2302.14172

Priorização de *Patches* com Base em Risco

Risco = Vulnerabilidade + Ameaça + Impacto

Queremos responder essa pergunta:

Qual o risco de uma vulnerabilidade
ser ativamente explorada **e** causar um impacto negativo?

Ou seja, **quais patches** eu preciso **aplicar agora e quais podem esperar** a próxima janela de manutenção?

TL;DR:

Risco = Vulnerabilidade + Ameaça + Impacto

CVSS COMMON VULNERABILITY SCORING SYSTEM + CISA KEV e EPSS Exploit Prediction Scoring System + SSVC

Alguns Padrões para Informar as Decisões de Risco: CVSS, CISA KEV, EPSS e SSVC

TLP:CLEAR

CVSS – *Common Vulnerability Scoring System*

– Uma pontuação relativa à **severidade** de uma vulnerabilidade
  - ex: execução remota de código sem interação vs. necessidade de conta no sistema para posterior escalação de privilégio

EPSS – *Exploit Prediction Scoring System*

– **Probabilidade de** uma vulnerabilidade **ser ativamente explorada** nos próximos 30 dias

SSVC – *Stakeholder-Specific Vulnerability Categorization*

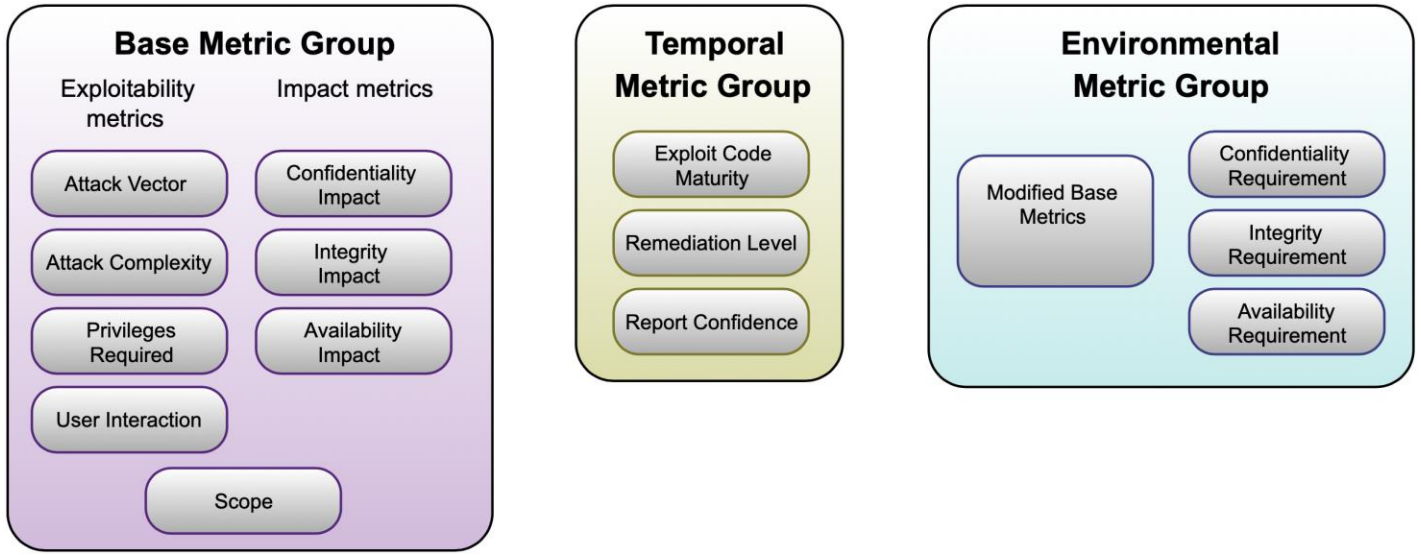
– Uma **metodologia para priorizar** vulnerabilidades com base nas necessidades das partes interessadas
  - Criada pelo CERT Division SEI/CMU em conjunto com a CISA
  - CISA instituiu um processo específico para o Governo dos EUA
  - **CISA** criou a base **KEV (*Known Exploited Vulnerabilities*)** como parte deste esforço

CVSS v3.1

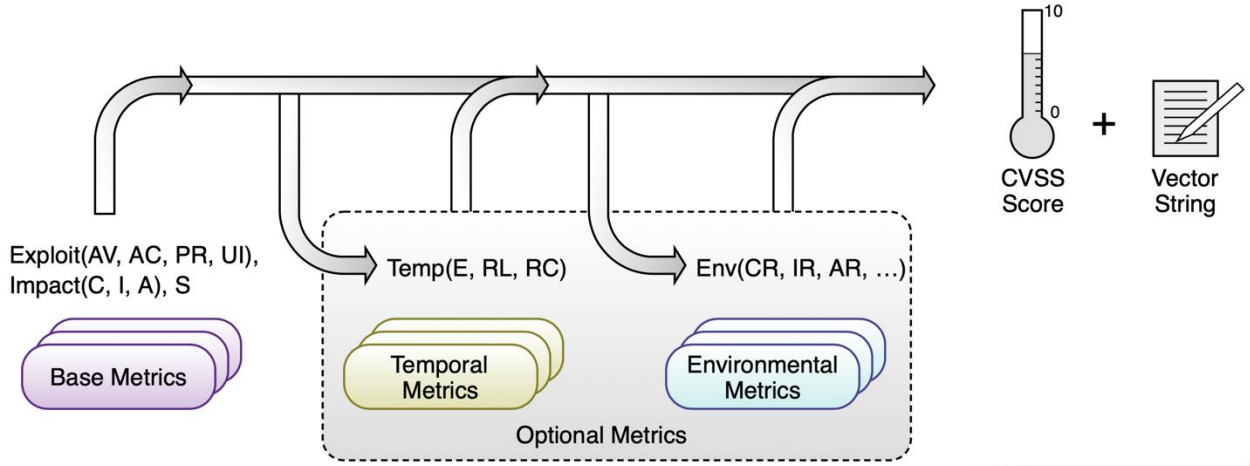
TLP:CLEAR

"The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities."

CVSS Metric Groups



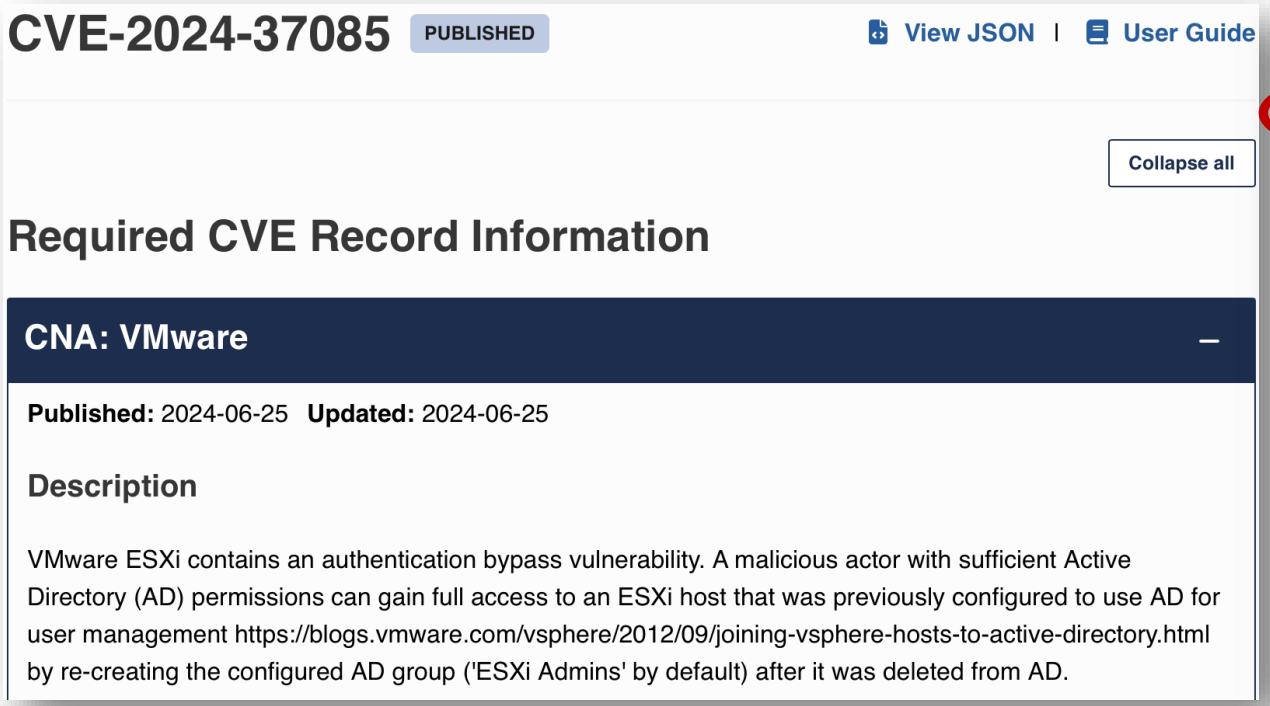
CVSS Metrics and Equations



Fonte: https://www.first.org/cvss/

Exemplo: CVE-2024-37085 (VMware ESXi)
Registro CVE com Escore CVSS Calculado

TLP:CLEAR



CVE-2024-37085 PUBLISHED

View JSON | User Guide

Collapse all

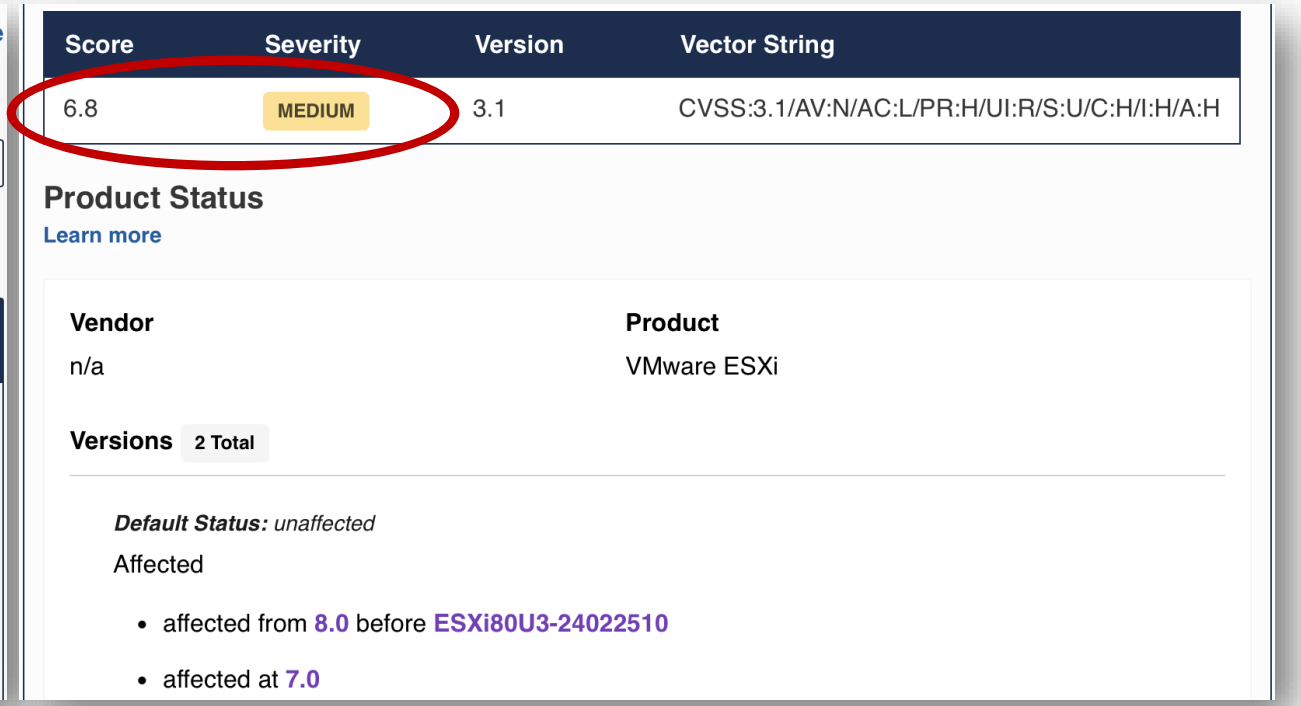
Required CVE Record Information

CNA: VMware

Published: 2024-06-25 **Updated:** 2024-06-25

Description

VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management https://blogs.vmware.com/vsphere/2012/09/joining-vsphere-hosts-to-active-directory.html by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.



Score	Severity	Version	Vector String
6.8	MEDIUM	3.1	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H

Product Status

Learn more

Vendor
n/a

Product
VMware ESXi

Versions 2 Total

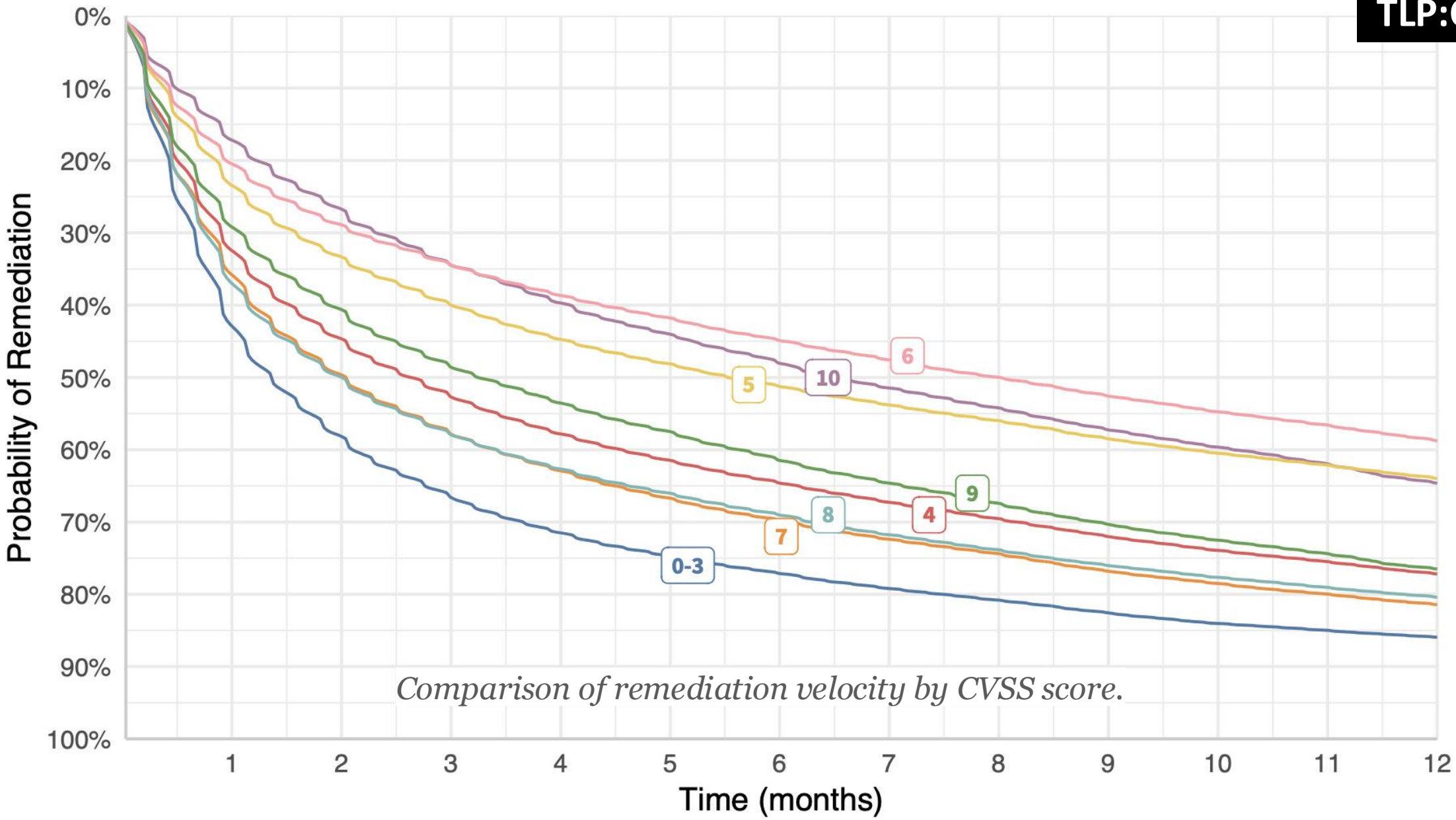
Default Status: *unaffected*

Affected

- affected from 8.0 before ESXi80U3-24022510
- affected at 7.0

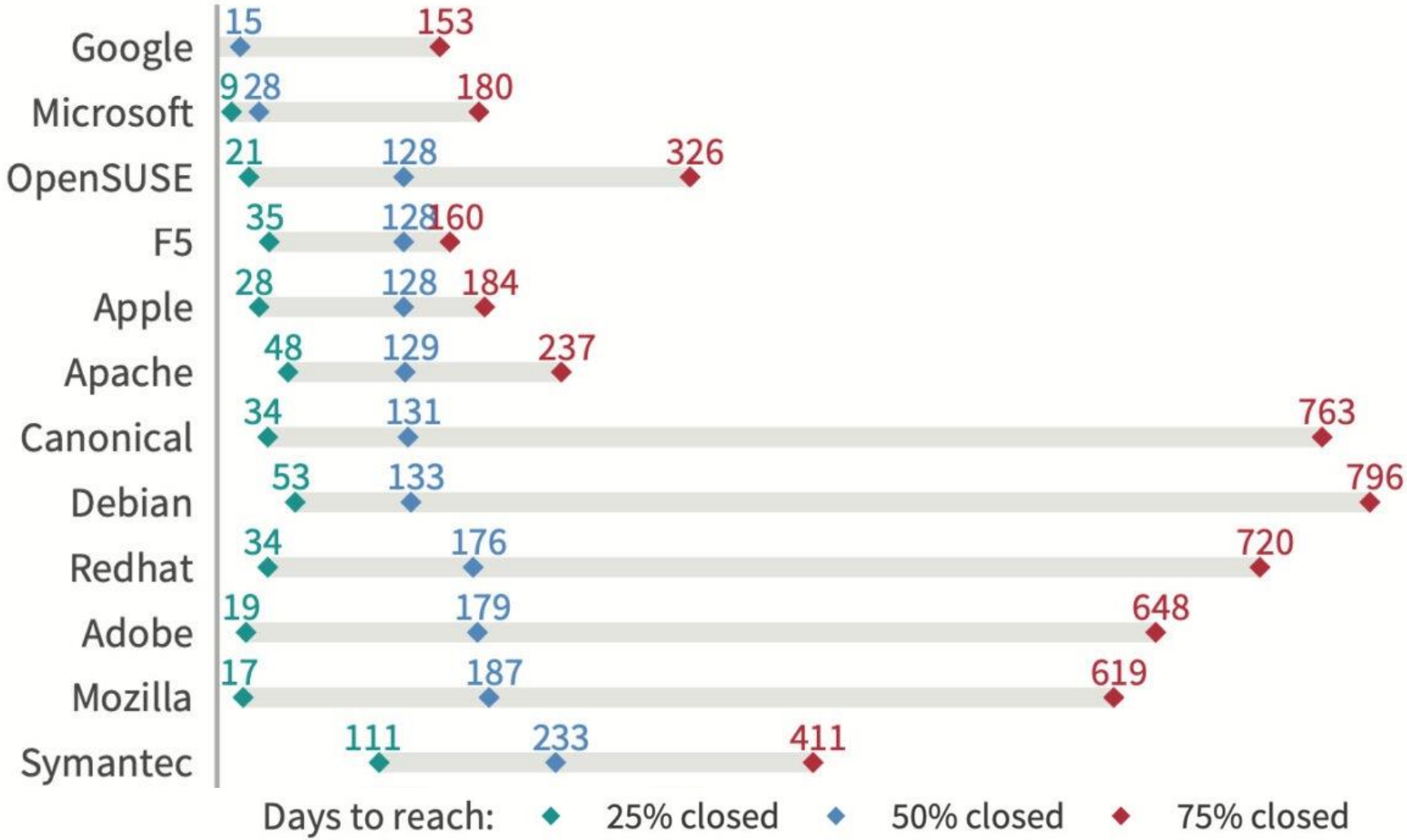
Fonte: https://www.cve.org/CVERecord?id=CVE-2024-37085

TLP:CLEAR



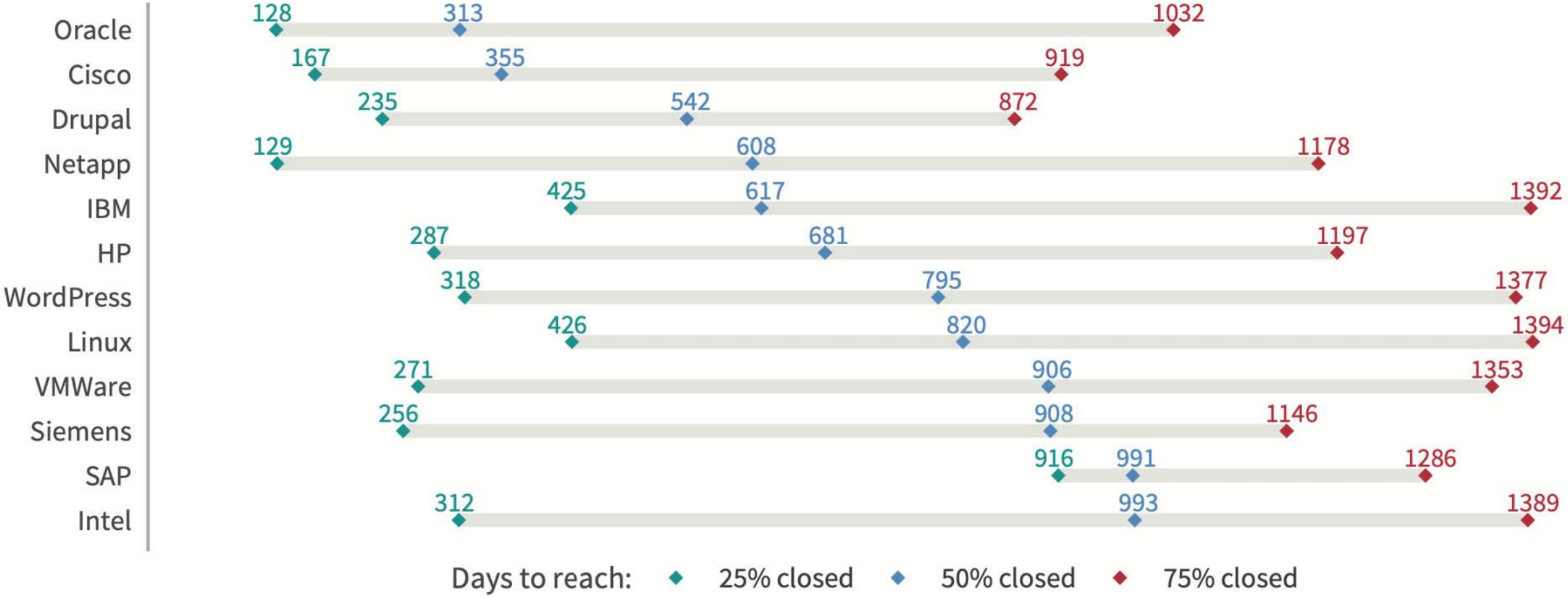
Comparison of remediation velocity by CVSS score.

Fonte: https://www.cyentia.com/patching-fast-and-slow/



Comparing remediation velocity for major product vendors (1/2)

Fonte: https://www.cyentia.com/patching-fast-and-slow/

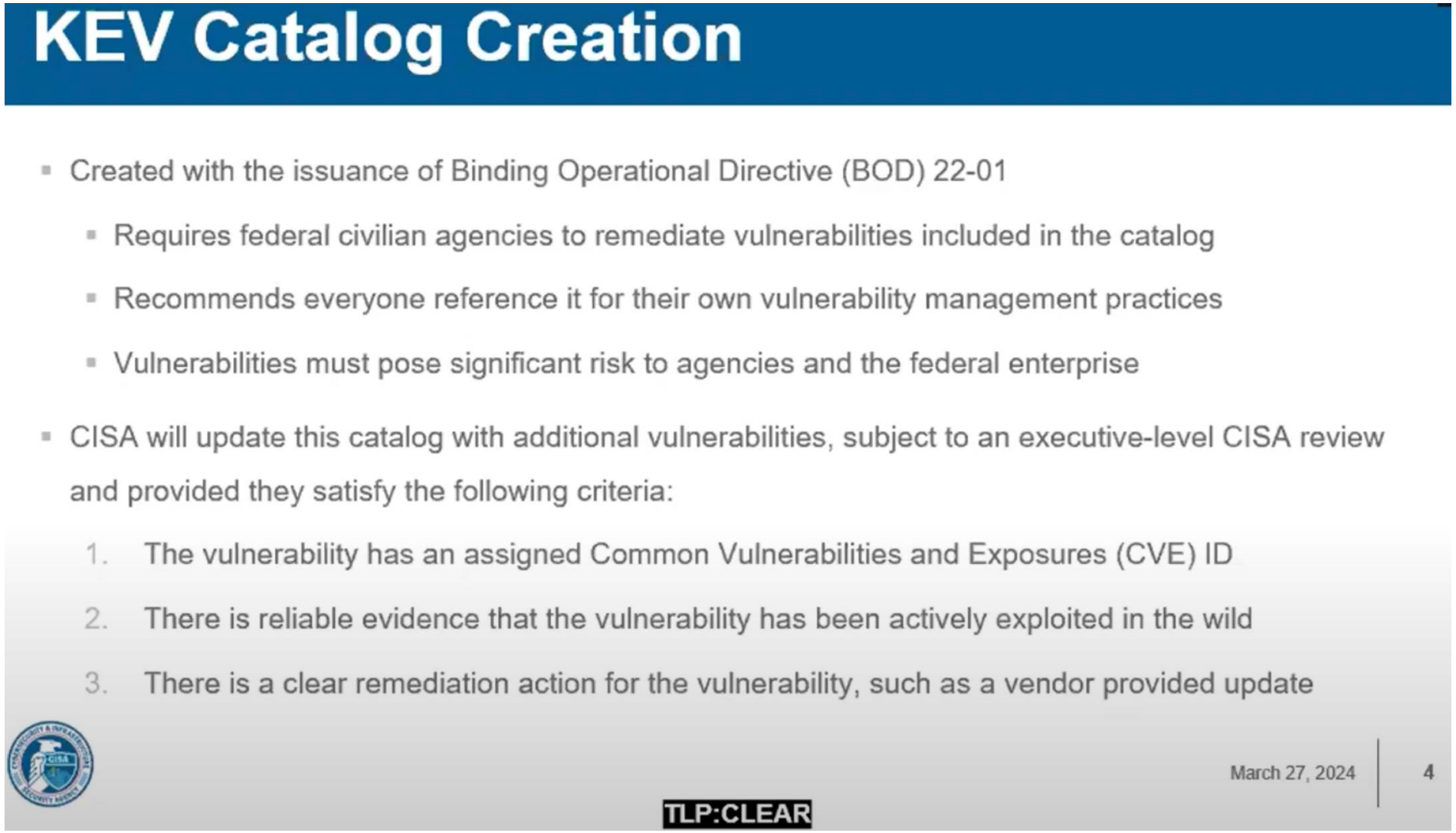


Comparing remediation velocity for major product vendors (2/2)

Fonte: https://www.cyentia.com/patching-fast-and-slow/

CISA KEV – *Known Exploited Vulnerabilities*

TLP:CLEAR



Fonte: CISA's Known Exploited Vulnerabilities (KEV) Catalog, CVE/FIRST VulnCon 2024 & Annual CNA Summit
https://youtu.be/T4kYHm54SM0?feature=shared&t=210

Exemplo: CVE-2024-37085 (VMware ESXi)
Informações Disponíveis no CISA KEV

TLP:CLEAR

Mesmo o CVSS sendo “só” 6.8, está sendo ativamente explorado (inclusive por *Ransomware*)

CVE-2024-37085

VMware ESXi Authentication Bypass Vulnerability: *VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.*

Related CWE: CWE-305

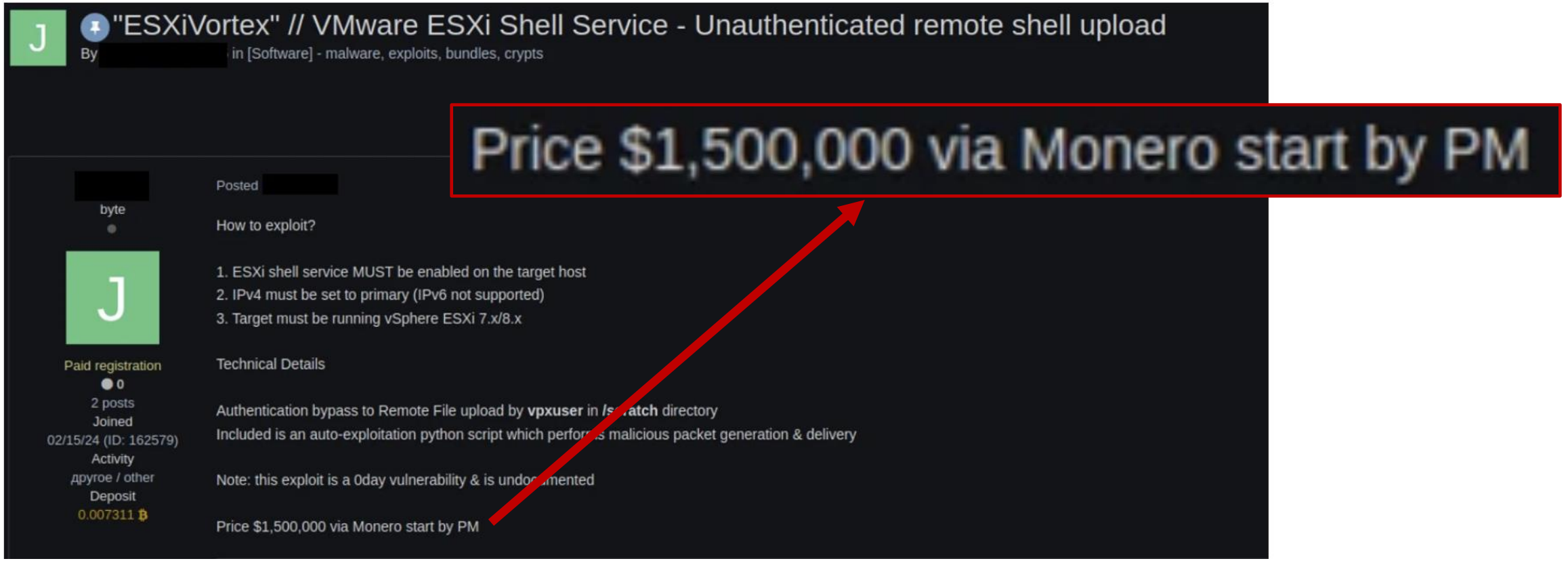
Known To Be Used in Ransomware Campaigns? **Known**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-07-30
- **Due Date:** 2024-08-20

Fonte: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-37085

Therefore, many ransomware threat actors like Storm-0506, Storm-1175, Octo Tempest, Manatee Tempest, and others support or sell ESXi encryptors like Akira, Black Basta, Babuk, Lockbit, and Kuiper (Figure 1). The number of Microsoft Incident Response (Microsoft IR) engagements that involved the targeting and impacting ESXi hypervisors have more than doubled in the last three years.



Fonte: https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/

Mas, se ainda não estiver no KEV, como estimar se tem chance de ser explorado?

https://www.first.org/epss/

“The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild.”

– Objetivo: ajudar as organizações a terem a melhor cobertura de aplicação de patches com o menor esforço (já que recursos são limitados)

– Dados levados em conta para o cálculo da pontuação: Idade do CVE, CPE, CWE, CVSS 3.x, CISA KEV, Google Project Zero, Trend Micro's Zero Day Initiative (ZDI), Exploit-DB, GitHub, MetaSploit, Intrigue, sn1per, jaeles, nuclei, entre outros

– Quem usa:
  - https://www.first.org/epss/who_is_using/

– Ferramentas Open Source:
  - https://www.first.org/epss/epss_tools

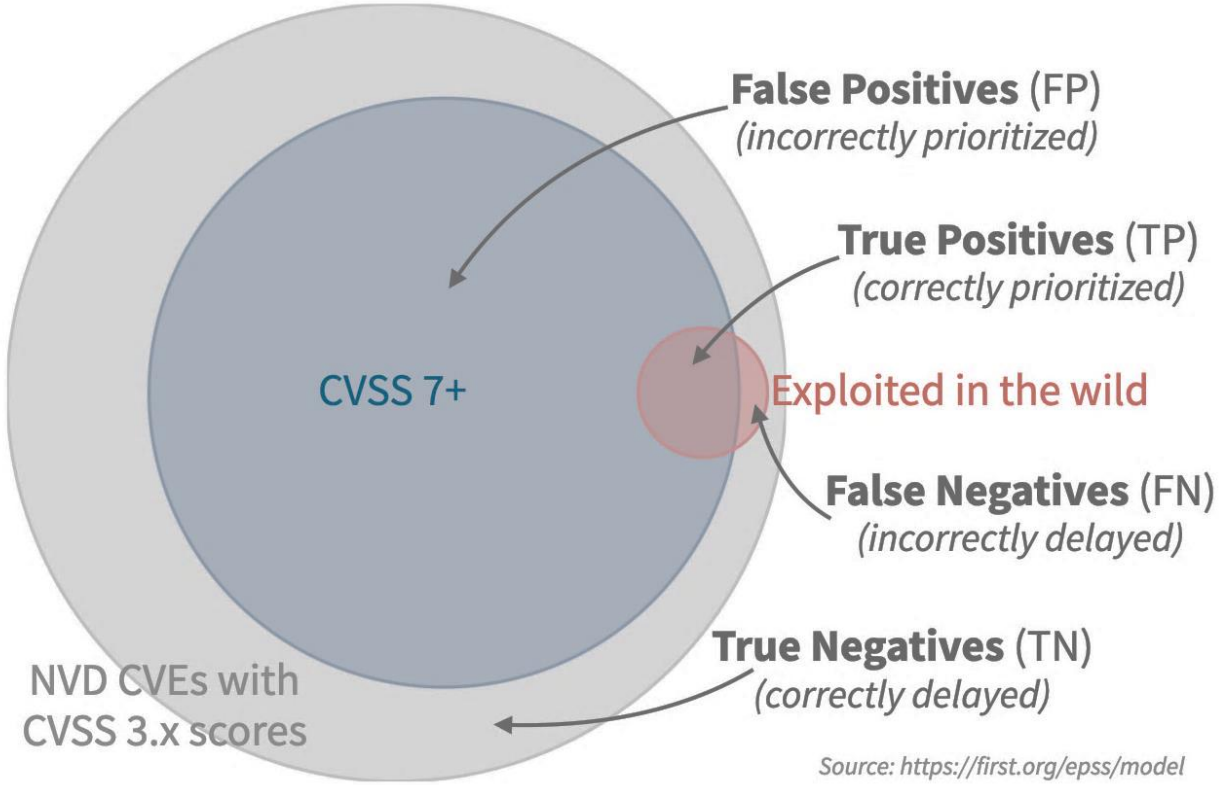
– Dados completos – arquivo CSV atualizado diariamente:
  - https://www.first.org/epss/data_stats

Efetividade do EPSS na Vida Real

Metodologia

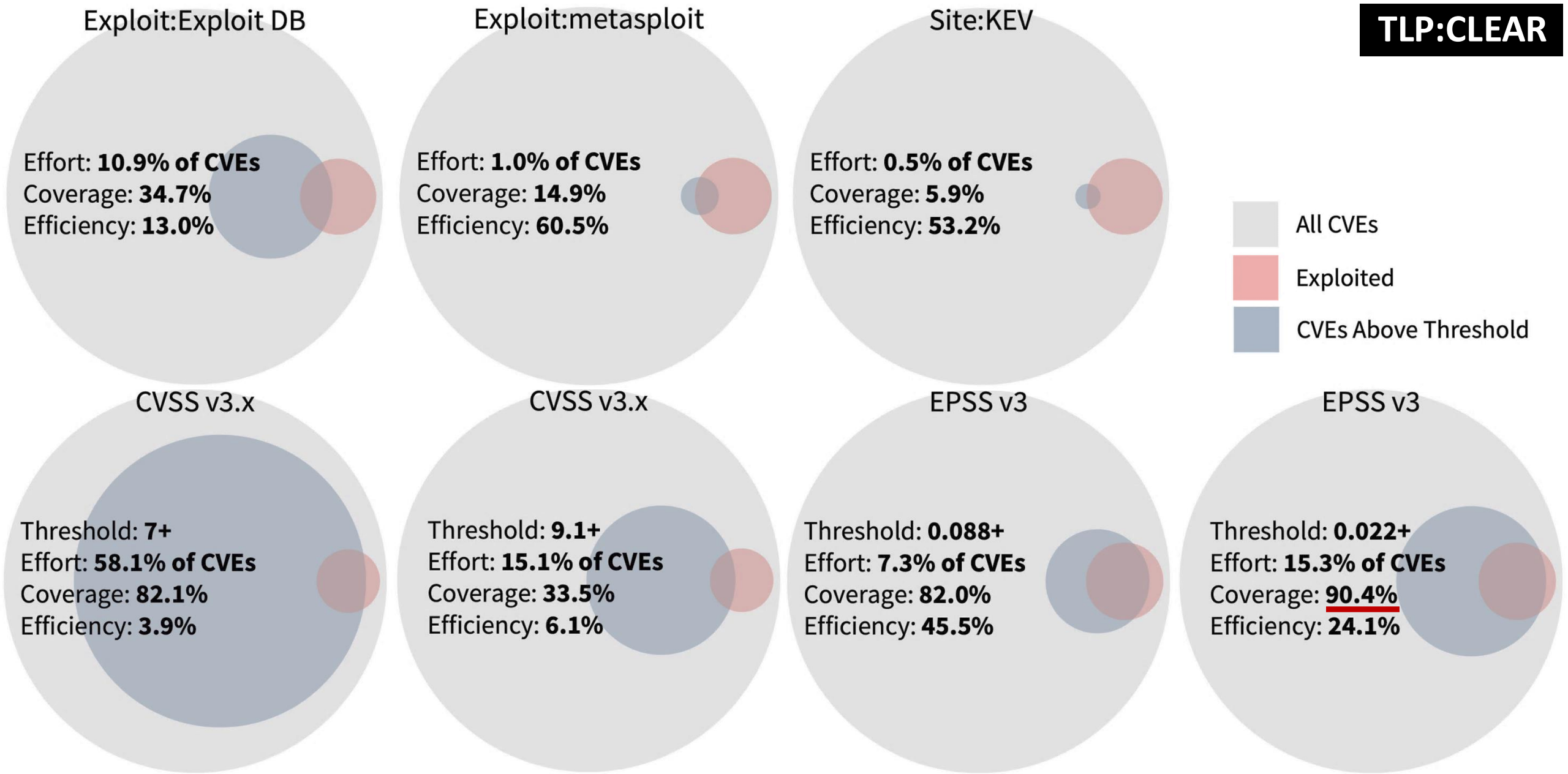
- 1 ano de dados usados para treinar o modelo
  - CVEs publicados entre 01/11/2021 – 31/10/2022
- Período de teste: dezembro/2022
- Avaliar para este mês
  - predições do EPSS versus
  - outras estratégias de priorização

Entendendo os Gráficos do próximo *slide*



Fonte: https://arxiv.org/pdf/2302.14172

TLP:CLEAR



Fonte: https://arxiv.org/pdf/2302.14172

Mas ainda assim são muitas vulnerabilidades,

tem como refinar mais?

SSVC - Stakeholder-Specific Vulnerability Categorization

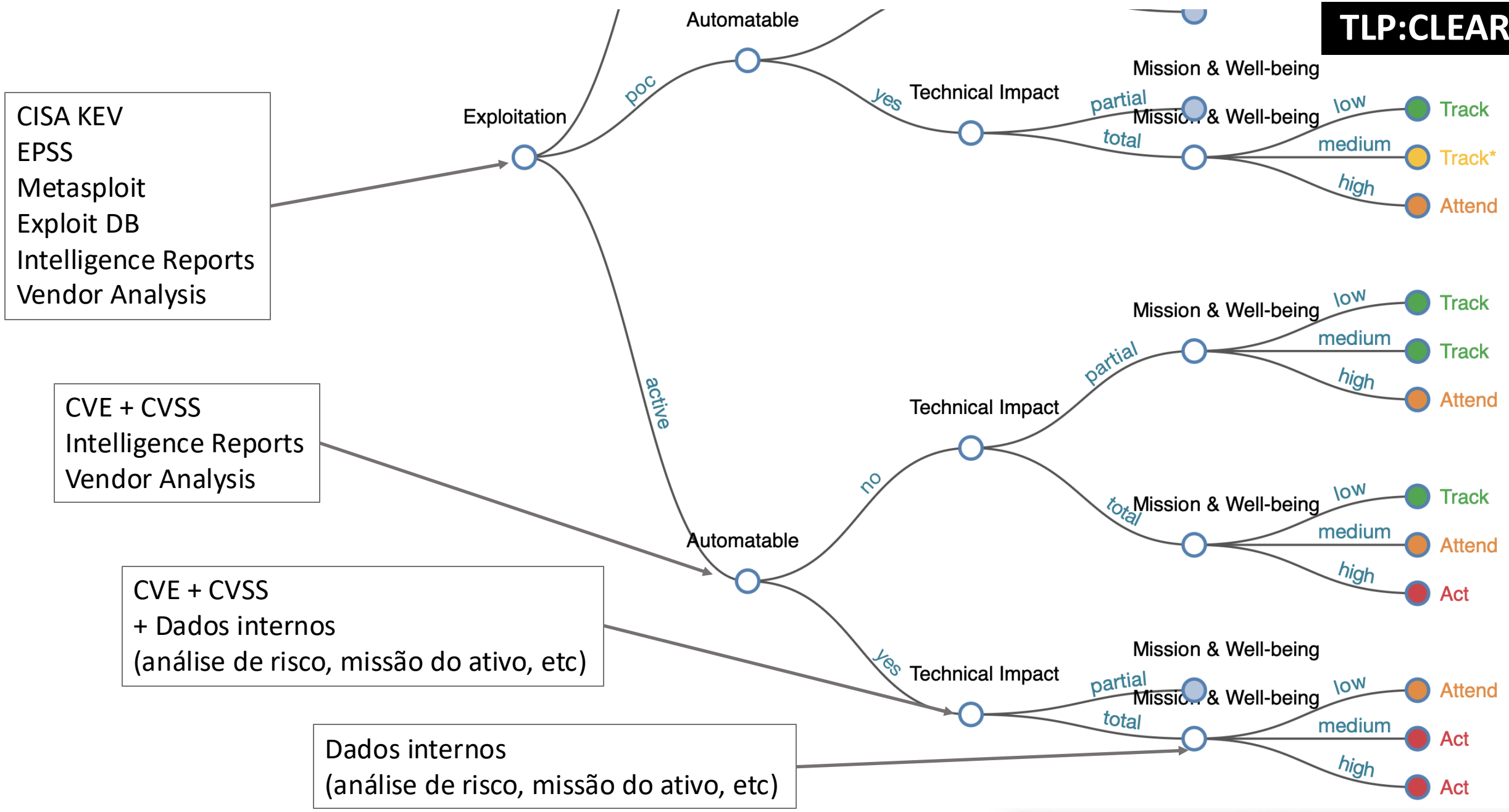
– Uma árvore de decisão, que leva em conta as seguintes propriedades:
  - Evidência de uma vulnerabilidade estar sendo ativamente explorada
  - Impacto técnico
  - Se o ataque é automatizável
  - Impacto na missão e no bem-estar social

– Relação com CVSS e EPSS
  - CVSS pode ser usado para informar a decisão de impacto técnico
  - EPSS pode ser usado para decidir a probabilidade e/ou evidência de estar sendo ativamente explorado

Prioridade	Descrição
Track	Não requer atenção neste momento
Track*	Corrigir na próxima janela de manutenção
Attend	Corrigir mais cedo que o normal
Act	Corrigir imediatamente

Fontes:
CISA SSVC – https://www.cisa.gov/ssvc/
Learning SSVC – https://certcc.github.io/SSVC/tutorials/
Stakeholder-Specific Vulnerability Categorization (SSVC), Technical Report
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379

TLP:CLEAR


CISA KEV
EPSS
Metasploit
Exploit DB
Intelligence Reports
Vendor Analysis
CVE + CVSS
Intelligence Reports
Vendor Analysis
CVE + CVSS
+ Dados internos
(análise de risco, missão do ativo, etc)
Dados internos
(análise de risco, missão do ativo, etc)
Exploitation
poc
Automatable
yes
Technical Impact
partial
total
Mission & Well-being
low
medium
high
Track
Track*
Attend
active
Automatable
no
Technical Impact
partial
total
Mission & Well-being
low
medium
high
Track
Track
Attend
Automatable
yes
Technical Impact
partial
total
Mission & Well-being
low
medium
high
Track
Attend
Act
Mission & Well-being
low
medium
high
Attend
Act
Act

Recomendações

Assuma o Controle da Priorização da Aplicação de Patches

Quem assume o risco, em última instância, é você e sua organização

– Não use apenas CVSS como critério

– Cobre seu fornecedor de ferramentas de gestão de vulnerabilidades
  - Desconfie se a resposta for muito simplista
  - É OK ter uma solução própria, mas é necessário saber algo sobre quais métricas são usadas
  - Verifique se ele já não integra EPSS e/ou SSVC

– Complemente com sua própria avaliação
  - Os dados são todos públicos

Implemente a RFC 9116 e tenha em seu site o security.txt:
`https://<seu-site>/.well-known/security.txt`

`https://securitytxt.org/`

Considerações Finais

– Diversas vulnerabilidades estão sendo ativamente exploradas

– Ataques são capazes de falir sua empresa ou impedir serviços ao cidadão

– Sim, é difícil instalar todos os patches
  - entre outras coisas, falta tempo e pessoal capacitado

– Mas é preciso identificar os patches imprescindíveis
  - “É pra ontem”
    - Se estiver no CISA KEV
    - Se o CERT.br te notificar
  - É para fazer assim que possível
    - Se o EPSS estiver alto
    - Se for ativo que se parar, impede sua organização de funcionar

Isso é tudo que existe nessa área?

cert.br nic.br cgi.br


EPSS
CVSS
CWE
NVD
SBOM
SSVC
VDP
VEX
CVD
CSAF
KEV
CNA
CVE

Fique de olho em *Coordinated Vulnerability Disclosure*
Já está sendo requerida por diversos padrões

TLP:CLEAR

- ISO/IEC 29147 and 30111
  https://webstore.ansi.org/standards/iso/isoiec3011129147security
- EthicsfIRST
  https://ethicsfirst.org/
- FIRST PSIRT and CSIRT Services Frameworks
  https://www.first.org/standards/frameworks/
- Políticas da OECD e da União Europeia
  https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482
  https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu
- IETF security.txt – *RFC 9116: A File Format to Aid in Security Vulnerability Disclosure*
  https://securitytxt.org
- Ato nº 77 da Anatel, Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações, seção 6.1.6
  https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77

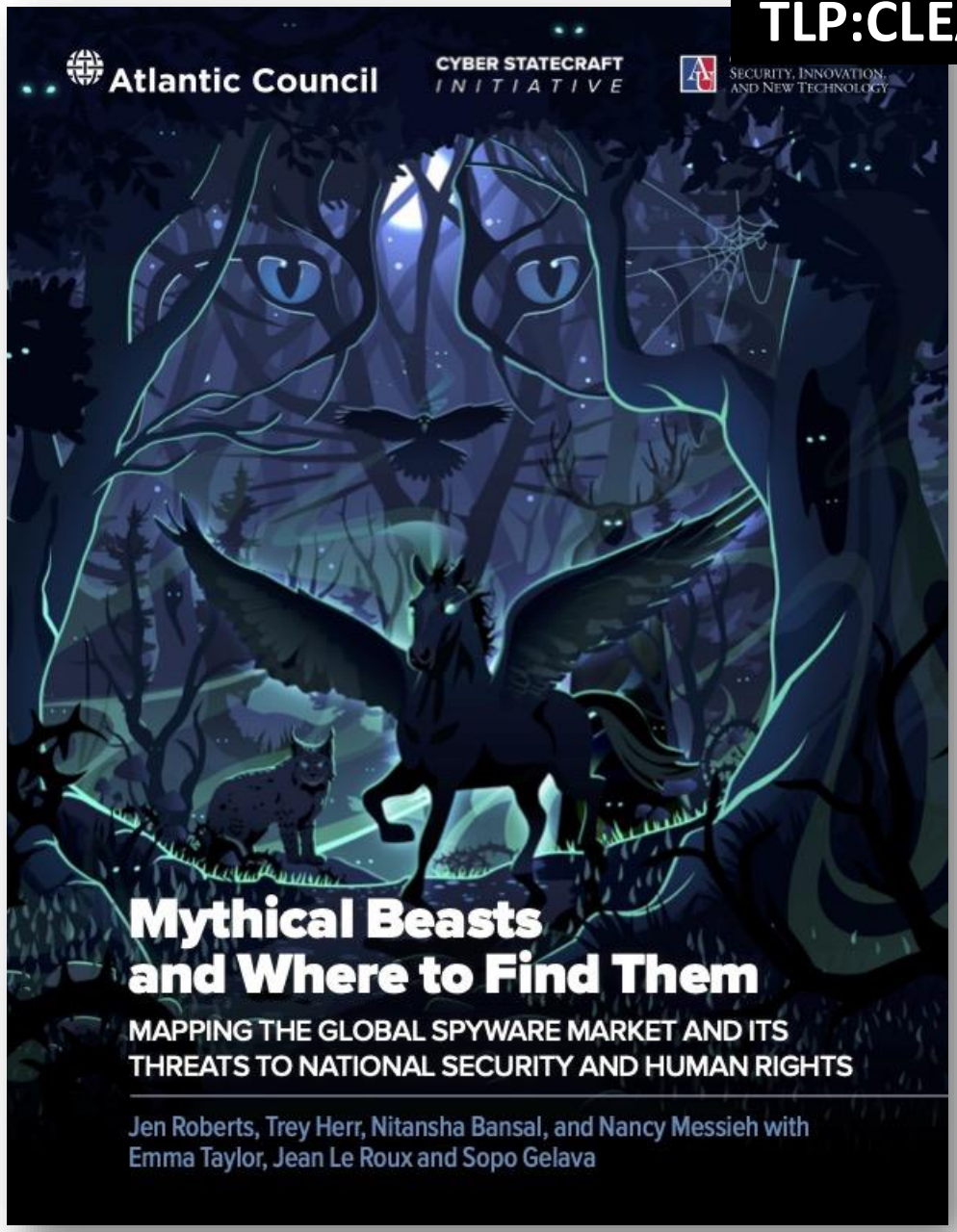
Referências Adicionais

- Software Bill of Materials (SBOM)
  https://www.cisa.gov/sbom
- CERT.br – Estatísticas de notificações de dispositivos com serviços potencialmente vulneráveis expostos na Internet
  https://stats.cert.br/vulns/
- CVE/FIRST VulnCon 2024 & Annual CNA Summit
  Slides: https://www.first.org/conference/vulncon2024/program
  Vídeos:
  https://youtube.com/playlist?list=PLBAUUhONOrO_aB01lOv6XNRTHD4ueFVTp&feature=shared
- Obsolescência não-Programada: Análise do Uso de Software Desatualizado em Ambiente de Produção, Luan Marko Kujavski, Ulisses Penteado, Paulo Lisboa de Almeida, André Grégio, SBSeg 2024
  https://sol.sbc.org.br/index.php/sbseg/article/view/30046/29853
- CIRCL Vulnerability Lookup Tool – facilitates quick correlation of vulnerabilities from various sources, independent of vulnerability IDs, and streamlines the management of Coordinated Vulnerability Disclosure (CVD).
  https://github.com/cve-search/vulnerability-lookup

TLP:CLEAR

Informe-se mais sobre o Mercado Global de *Spyware* e Zero-Days

- Dos 195 países no mundo, pelo menos **80** compraram ***spyware*** de fabricantes comerciais
- 14 dos 27 países da União Europeia **compraram *spyware*** de um único fabricante, o ***NSO Group***.
- **Fabricantes de *Spyware*** são responsáveis pela maior parte dos 0-days descobertos em 2023:
  - **50% de todos os *0-days*** foram descobertos por uma única empresa, incluindo **64% de todos os *exploits* para navegadores e smartphones.**
  - Os principais fornecedores de 0-days para esses fabricantes são Zerodium, Aglaya e DarkMatter.



https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/

Obrigada

@ cristine@cert.br

@ Notificações para: cert@cert.br

https://cert.br

nic.br cgi.br

www.nic.br | www.cgi.br