Priorizando a Correção de Vulnerabilidades com Base em Contexto e Avaliação de Risco

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

26º WRNP – 19 de maio de 2025
Natal - RN

cert.br nic.br cgi.br

Gestão de Vulnerabilidades

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

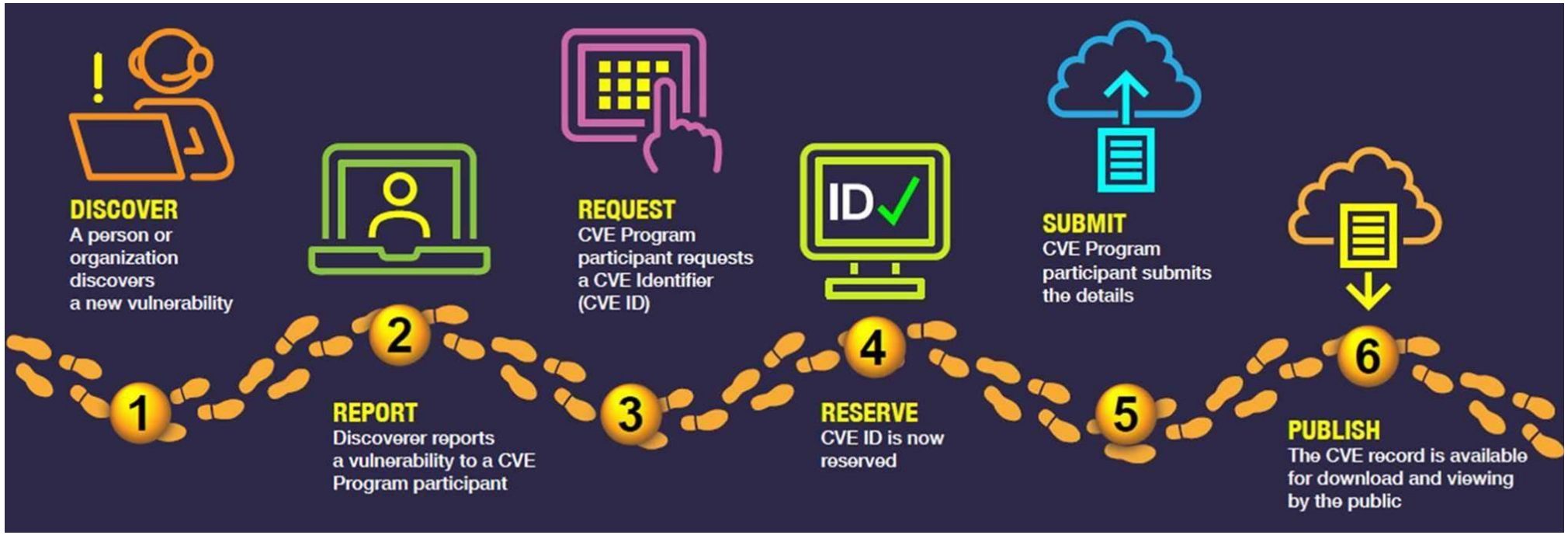
Fonte: https://arxiv.org/pdf/2302.14172

TLP:CLEAR

Alguns fatos sobre o *status* atual:
“Ou a Vulnerabilidade tem CVE ou não existe”

- Todas as ferramentas de gestão de *patches* dependem do CVE.
- A maioria consulta apenas o NVD para obter dados adicionais, como CVSS.

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

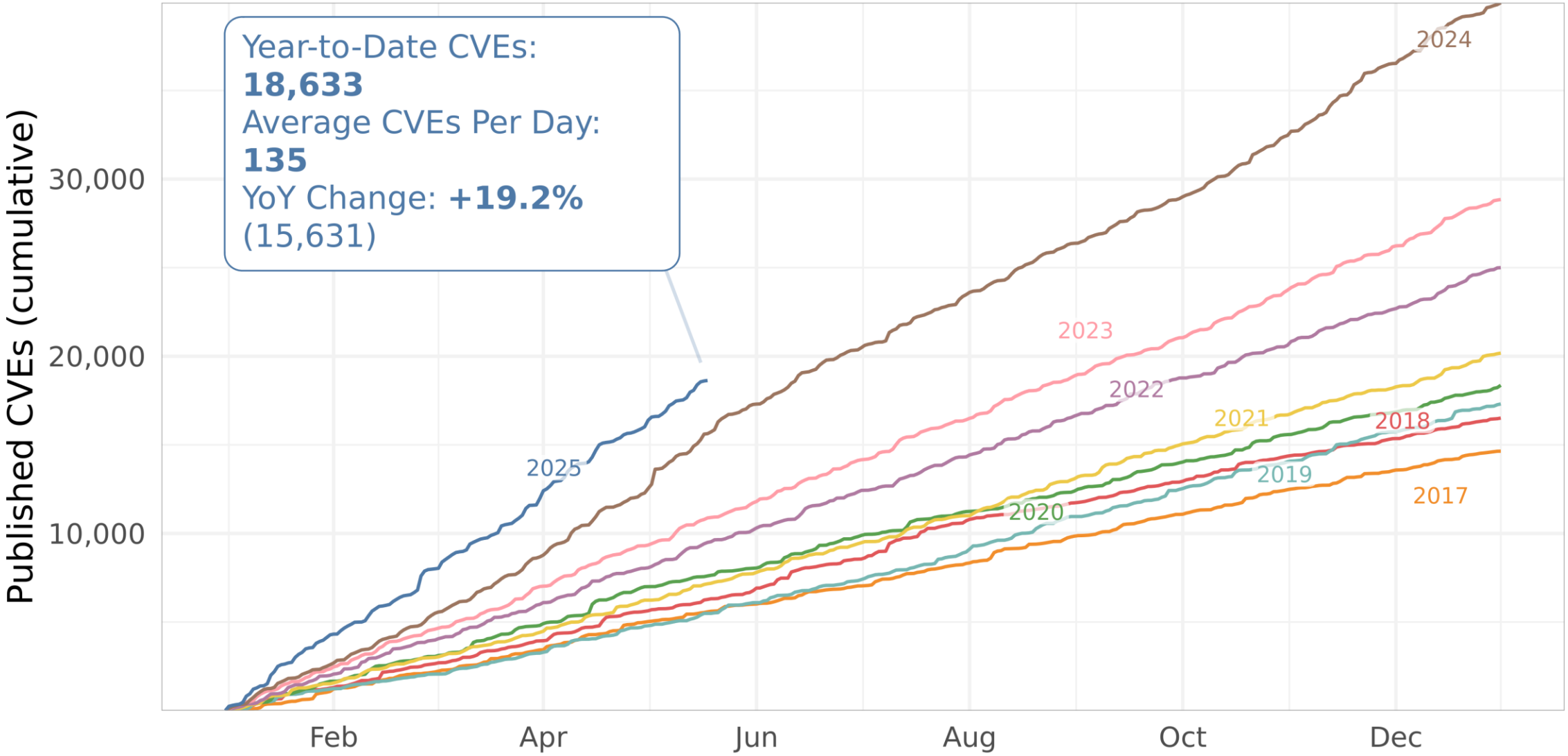


Fonte: https://www.cve.org/About/Process

TLP:CLEAR

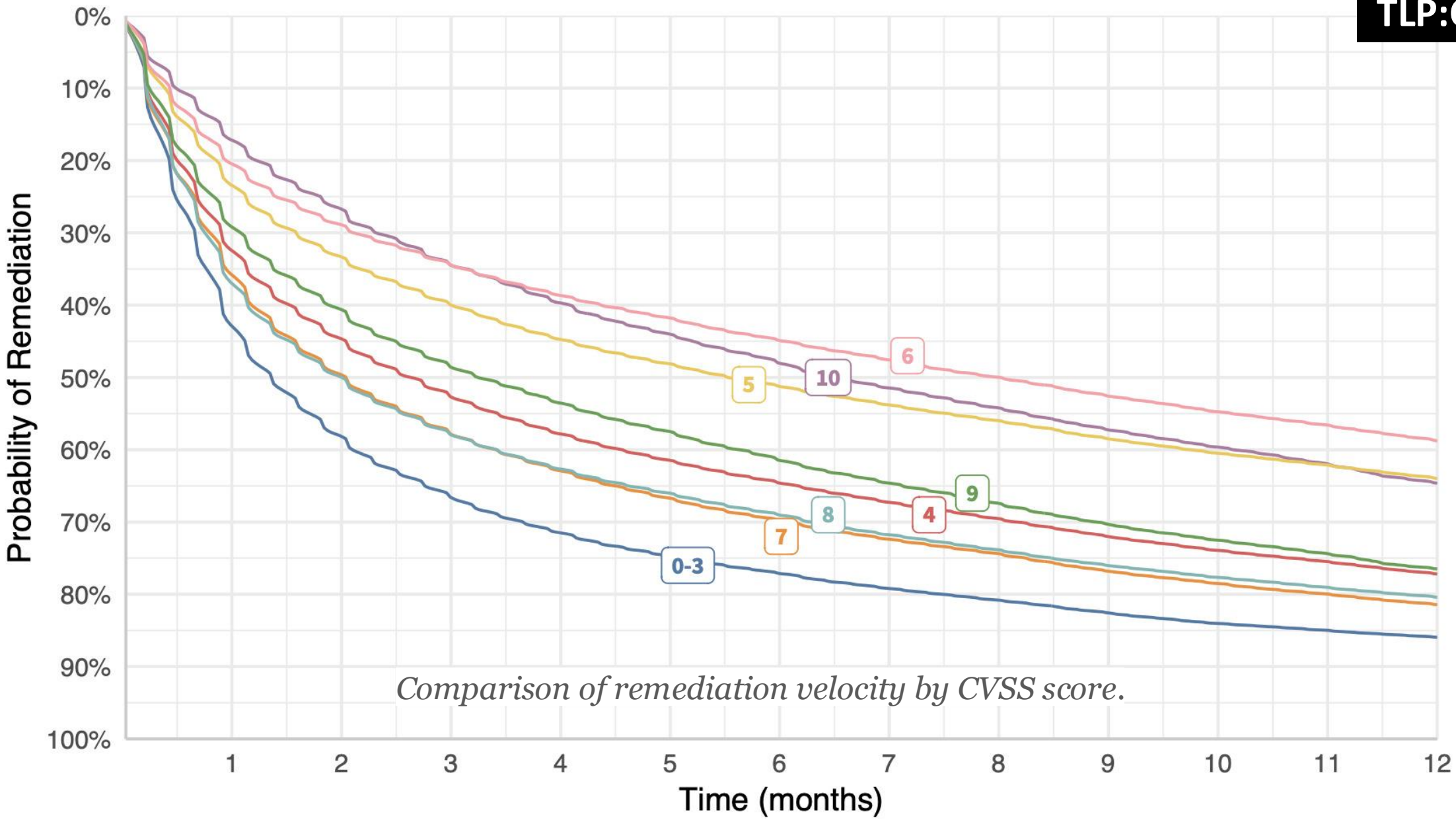
Year-to-date CVE publications (MITRE CVE List)

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



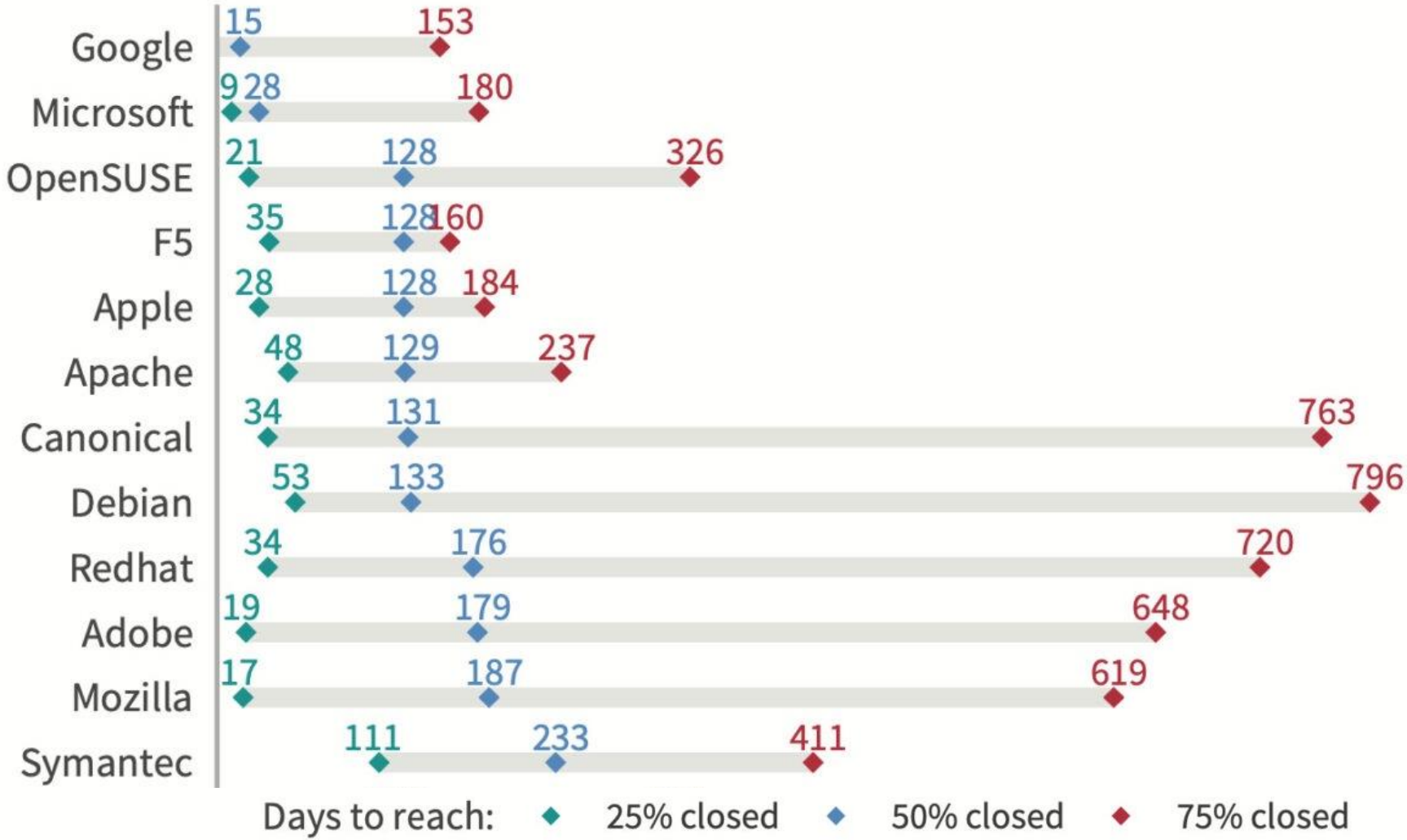
Fonte: https://www.first.org/epss/data_stats

Source: https://first.org/epss/data_stats, 2025-05-18



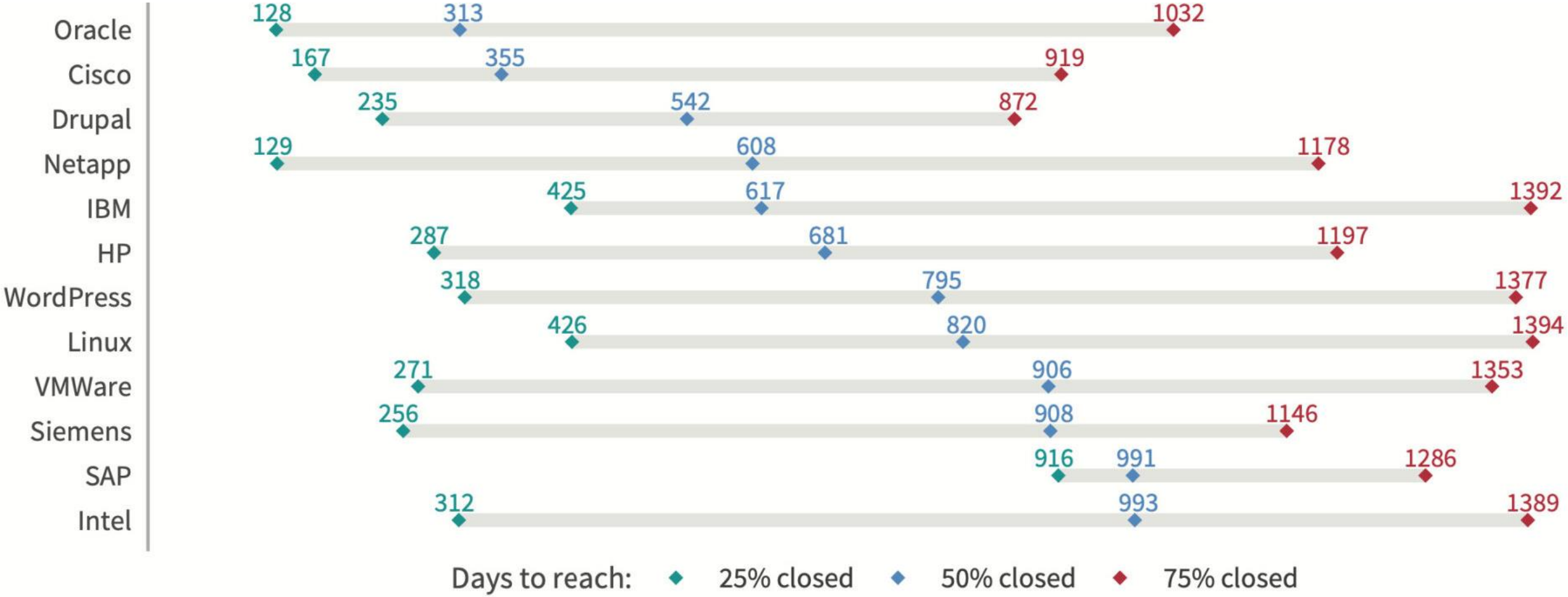
Comparison of remediation velocity by CVSS score.

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



Comparing remediation velocity for major product vendors (1/2) – "closed" = "patch applied"

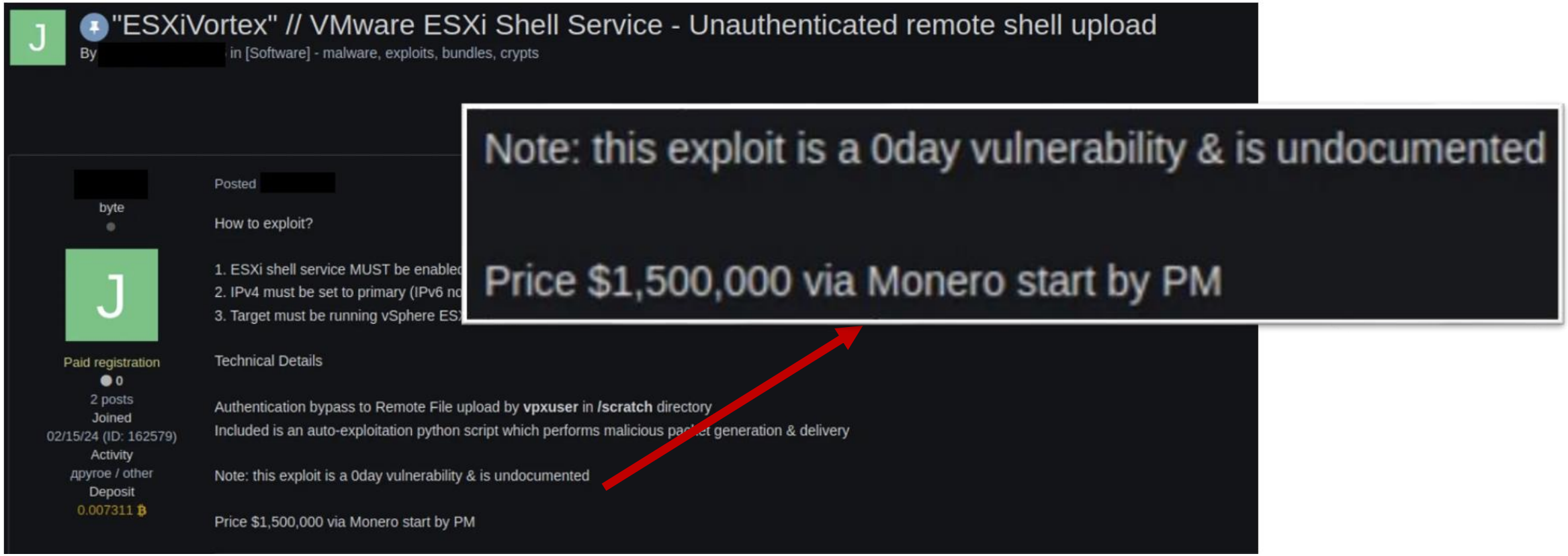
Fonte: https://www.cyentia.com/patching-fast-and-slow/



Comparing remediation velocity for major product vendors (2/2) – "closed" = "patch applied"

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

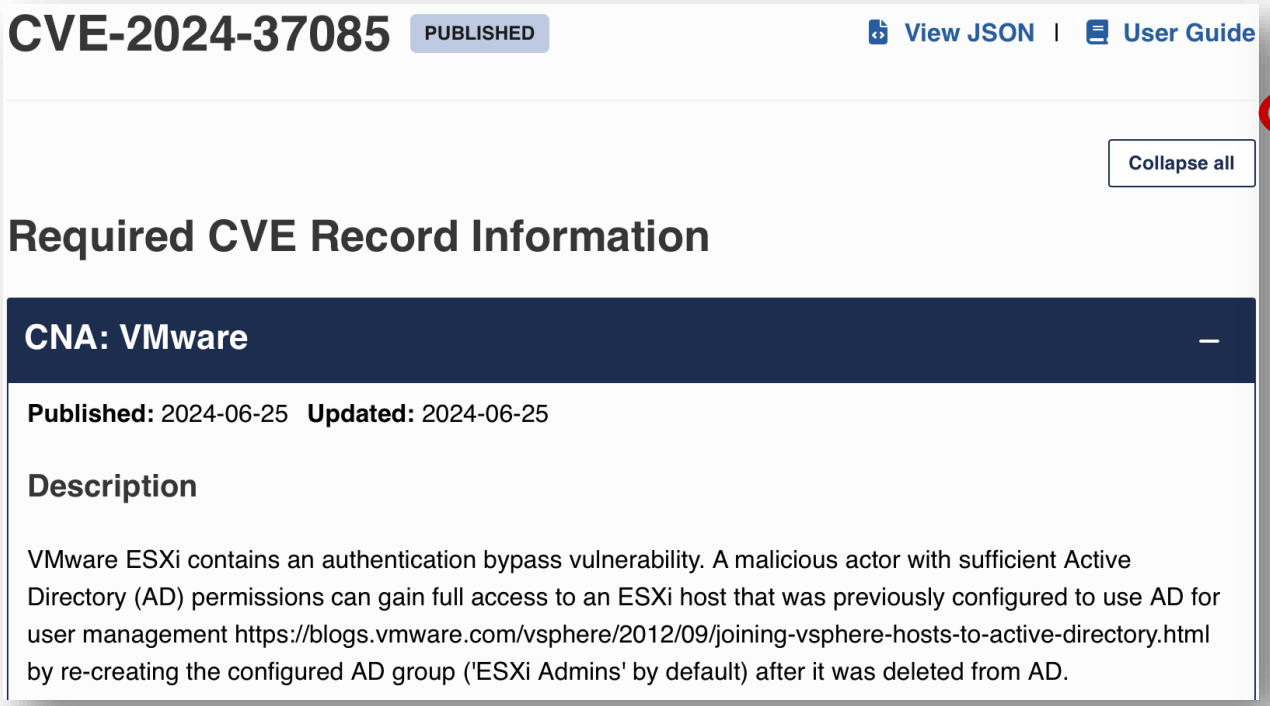
Therefore, many ransomware threat actors like Storm-0506, Storm-1175, Octo Tempest, Manatee Tempest, and others support or sell ESXi encryptors like Akira, Black Basta, Babuk, Lockbit, and Kuiper (Figure 1). The number of Microsoft Incident Response (Microsoft IR) engagements that involved the targeting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

Exemplo: CVE-2024-37085 (VMware ESXi) – 1
Escore CVSS Médio Não Significa que Não é Crítico

TLP:CLEAR



CVE-2024-37085 PUBLISHED

View JSON | User Guide

Collapse all

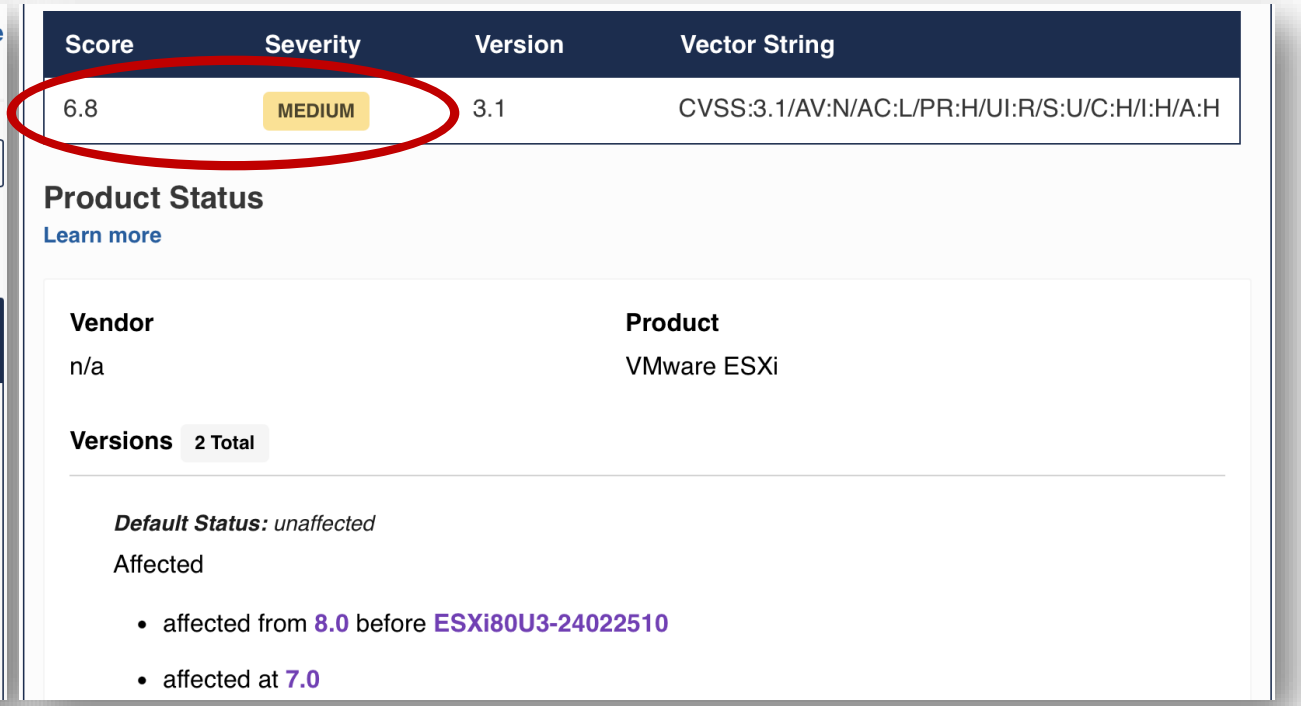
Required CVE Record Information

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

Exemplo: CVE-2024-37085 (VMware ESXi) – 2
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.

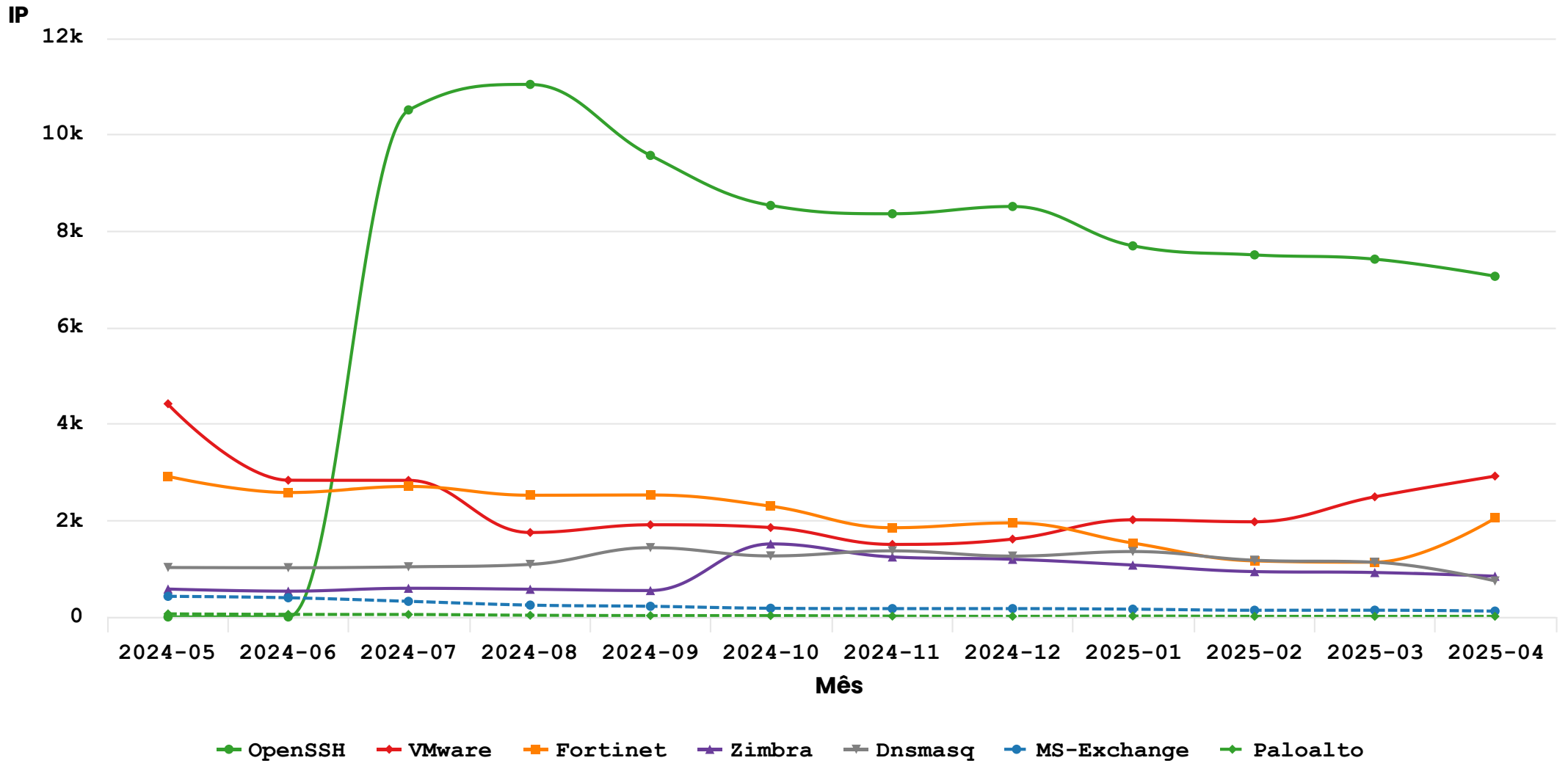
- **Date Added:** 2024-07-30
- **Due Date:** 2024-08-20

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

TLP:CLEAR

CERT.br notificações: endereços IP com servidores vulneráveis

2024-05 -- 2025-04



Endereços IP notificados pelo CERT.br – 36 CVE ao todo

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

Mais Algumas Estatísticas

- **Mais da metade** das organizações só conseguem **aplicar patches em 15.5%** dos CVEs/mês
  - ¼ corrige menos de 6.6% dos CVEs
- **Mas apenas 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

Priorização de *Patches* com Base em Risco

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?

É simples, mas não é fácil...

Risco = Vulnerabilidade + Ameaça + Impacto

+ CVSS + CISA KEV e EPSS + SSVC

CVSS
COMMON VULNERABILITY SCORING SYSTEM

EPSS
Exploit Prediction Scoring System

O CVSS dá uma nota para a vulnerabilidade sozinha, “no vácuo”. Não leva em conta o contexto:

- É explorável no contexto onde é usada?
- Tem mecanismos de proteção ou defesas no ambiente?
- Qual o impacto para mim?

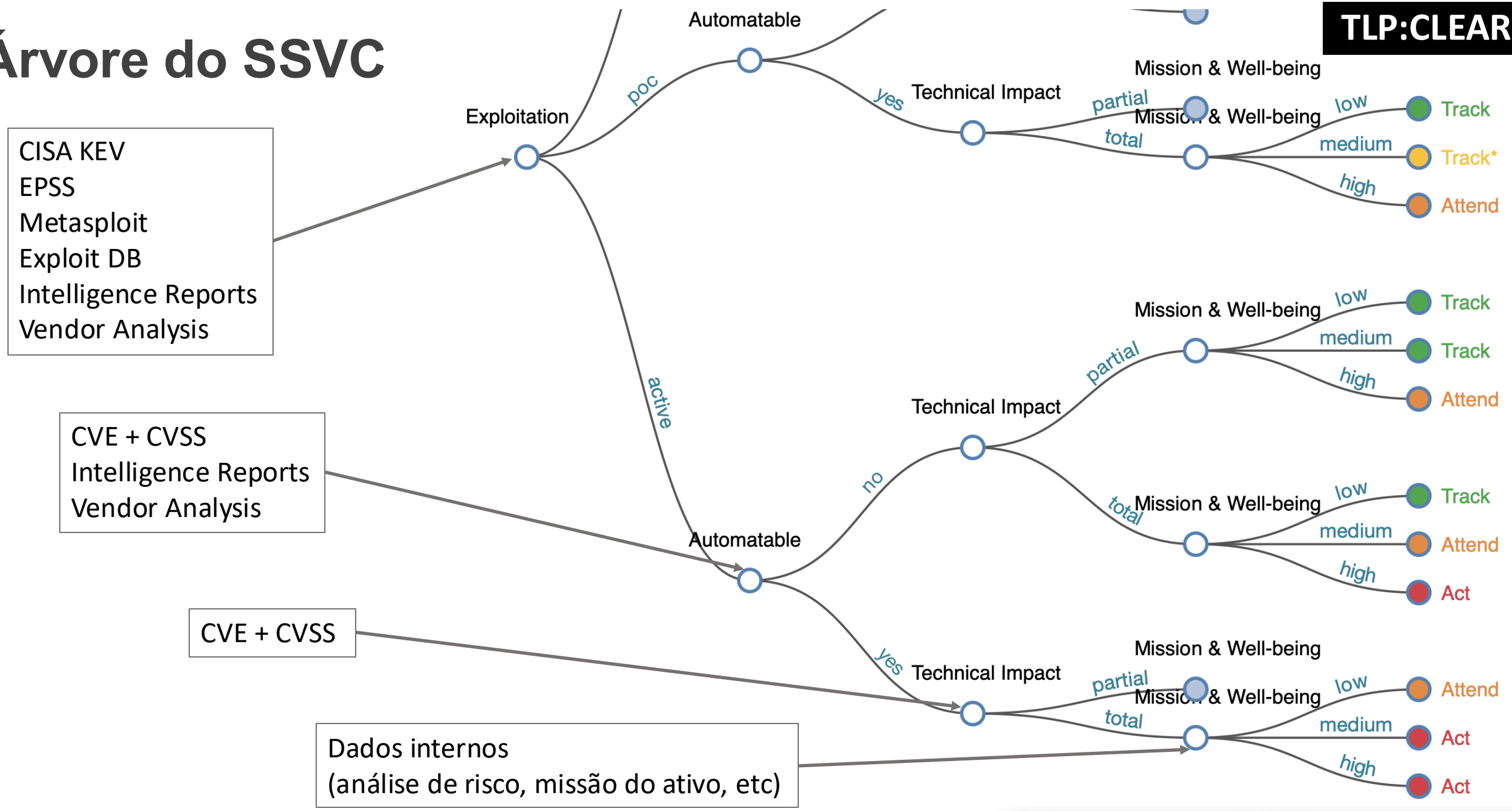
CISA KEV: “ground thruth”, mas limitado ao contexto do ambiente do público alvo do CISA.

EPSS: é uma previsão, como a do tempo, e podem ocorrer tempestades quando a previsão era de sol!

Requer conhecer em detalhes seu parque e ter um bom **mapeamento de ativos**, **versões**, **configurações** e uma boa **análise de risco**. **Você sabe**, mesmo, **todas as dependências** dos *softwares* que usa?

Árvore do SSVC

TLP:CLEAR

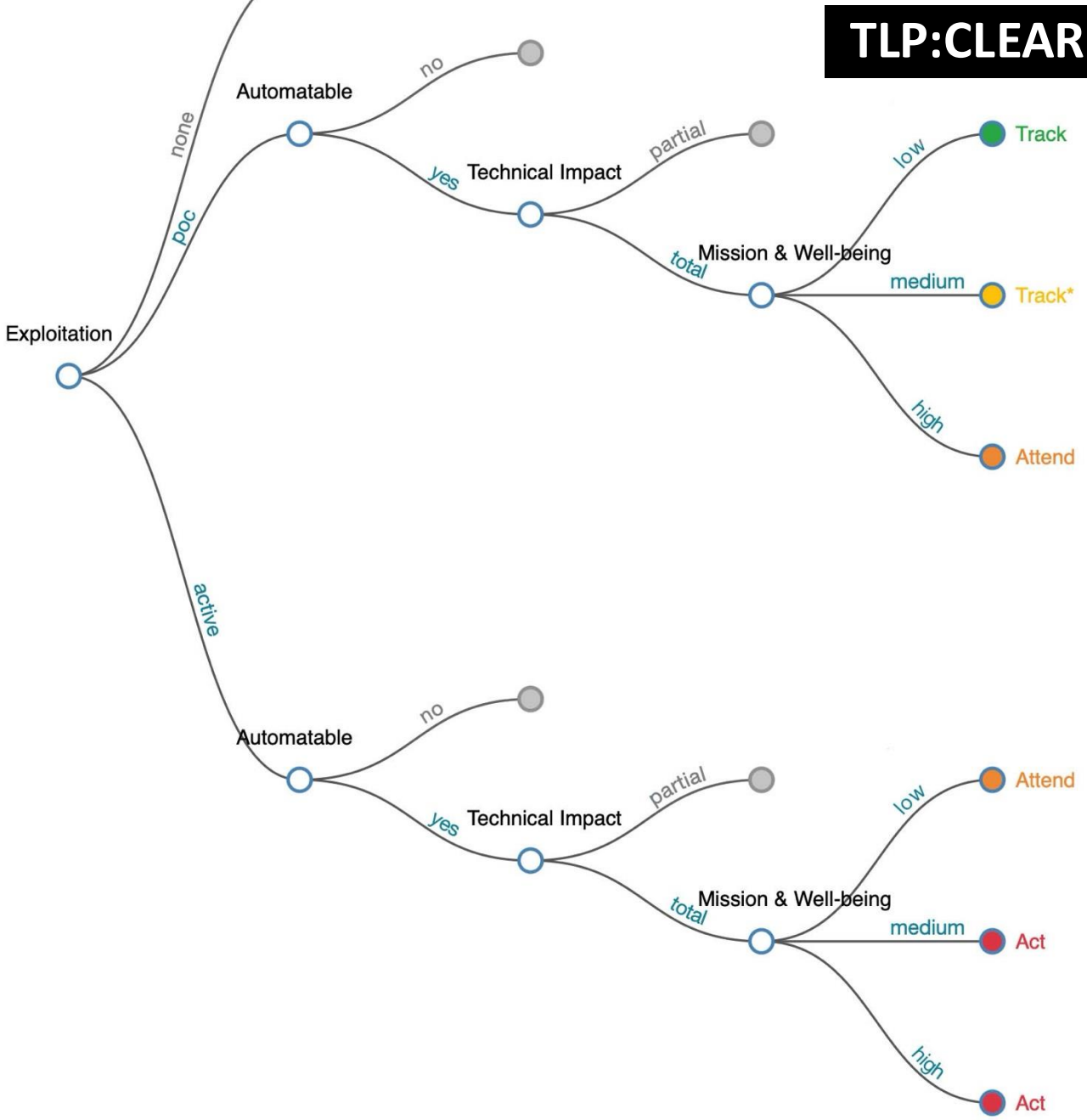


TLP:CLEAR

Making SSVC Easier: **CISA Vulnrichment**

– Agrupamento, em um único local, de informações sobre vulnerabilidades que preencham uma destas condições:
  - **`"Exploitation": ”yes”`**
  - **`"Exploitation": "poc”`**
  - **`"Automatable": "yes”`**
  - **`"Technical Impact": "total”`**

– Para cada CVE, o seu **`json`** passa a incluir os detalhes de:
  - CWE e CVSS



Fonte: https://github.com/cisagov/vulnrichment

Conhece-te a ti mesmo...

Para poder priorizar é necessário ter um mapeamento completo

- Análise de risco, aka, “Joias da Coroa”
  - tanto de dados, quanto de sistemas
- Determinar todas as versões de *software*
  - não é suficiente depender de banner de aplicação
  - precisa mapear também as dependências
- Não esquecer daquilo que é desenvolvido localmente
  - Bancos de dados, personalizações, APIs, aplicativos, etc, etc
  - Também é necessário mapear seus *frameworks*, pacotes e dependências
- Não esquecer da nuvem!

TLP:CLEAR

Para onde a Indústria e os Reguladores estão se movendo:
Requerer dos *Softwares* o seu SBOM e um Atestado VEX

Software Bill of Materials (SBOM)

- a nested inventory, a list of ingredients that make up software components
- identifies and lists software components, information about those components, and supply chain relationships between them

Software composition analysis (SCA)

- SCA tools identify all open-source packages in an application and all the known vulnerabilities of those packages.
- Software composition analysis tools can also be used to generate a software bill of materials (SBOM or software BOM) that includes all the open-source components used by an application.

Vulnerability Exploitability eXchange (VEX)

- a form of a security advisory that indicates whether a product is affected by a known vulnerability or vulnerabilities
- can support more effective use of SBOM data
- VEX documents are machine readable. The goal is to support greater automation across the vulnerability ecosystem, including disclosure, vulnerability tracking, and remediation

OASIS Common Security Advisory Framework (CSAF)

- a language to exchange Security Advisories
- automate the creation and consumption of security vulnerability information and remediation.

TLP:CLEAR

Esquemas para identificação unívoca de *software* e dependências:

O Ecossistema de Identificação de *Software*

– **CPE** – Common Platform Enumeration
  - a structured naming scheme for information technology systems, software, and packages.
  - **`cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:<target_hw>:<other>`**

– **PURL** – Package URL
  - ex: **`pkg:pypi/django@3.2.5. ; pkg:maven/org.apache.commons/commons-lang3@3.12.0 ; pkg:generic/libpng@1.6.37?download_url=https://sourceforge.net/projects/libpng/`**
    - **Type**: Indicates the package manager or ecosystem (e.g., npm, pypi, maven).
    - **Namespace**: Often represents the vendor or organization (e.g., apache for Apache projects).
    - **Name**: The name of the package.
    - **Version**: The version of the package (optional but recommended for specificity).
    - **Qualifiers**: Additional qualifiers for cases where more context is needed.
    - **Subpath**: Specifies a subpath within a larger package, if applicable.

– **OmniBOR**
  - Artifact ID – a SHA256 hash of the artifact
  - Input Manifest – a text file which records information about the inputs used to build a software artifacts. By "inputs" we mean anything provided to a build tool in order to produce the artifact.

Um Cenário Muito Melhor para Priorização

- Os seus sistemas terem um SBOM publicado
- O Vendor possuir um atestado VEX para todos os CVE publicados
- Os *scanners* de vulnerabilidades consumirem
  - os atestados VEX dos vendors
  - o SBOM do sistema como implantado no seu ambiente
  - um SSVC "base" ser criado ou vir de serviços como o CISA Vulnrichment
  - a ferramenta permitir incluir as **suas métricas** de "*Mission & Well-being*"

Exemplo: Vendors como RedHat já mantem atestados VEX:

"*The VEX file for a single, public CVE ID covers all the component statuses defined in the CSAF standard:*

- ***Fixed**: Contains the same fixed component versions and other details (product_tree objects) that the CSAF advisory reports for that CVE*
- ***Known Affected**: Confirmation that the specific component and product is affected by a particular CVE*
- ***Known Not Affected**: Confirmation that the specific component and product is not affected by a particular CVE*
- ***Under Investigation**: Information that the Red Hat Product Security team is verifying the applicability and impact of a specific CVE to the specific component and product*"

https://www.redhat.com/en/blog/red-hat-vex-files-cves-are-now-generally-available

O que fazer enquanto não vem a adoção ampla desses padrões?

cert.br nic.br cgi.br

Recomendações

É URGENTE conseguir identificar os patches imprescindíveis

- "É pra ontem"
  - Se o CERT.br notificar (https://stats.cert.br/vulns/)
  - Se estiver no CISA KEV (https://cisa.gov/kev/)
- Aplicar assim que possível
  - Se for em um ativo que se parar, impede sua organização de funcionar
  - Se atingir os critérios do CISA Vulnrichment (https://github.com/cisagov/vulnrichment)
  - Se o percentil do EPSS for muito alto (https://www.first.org/epss/)

Motivação

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

– Diversas vulnerabilidades antigas estão sendo ativamente exploradas

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

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, ele não foi feito para priorização!
  - vide *slide* anterior

– 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, cobre que consuma o VEX do fabricante

– 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/`

Obrigada

@ cristine@cert.br

@ Notificações para: cert@cert.br

https://cert.br

nic.br cgi.br

www.nic.br | www.cgi.br

Apêndice e Referências

cert.br nic.br cgi.br

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*

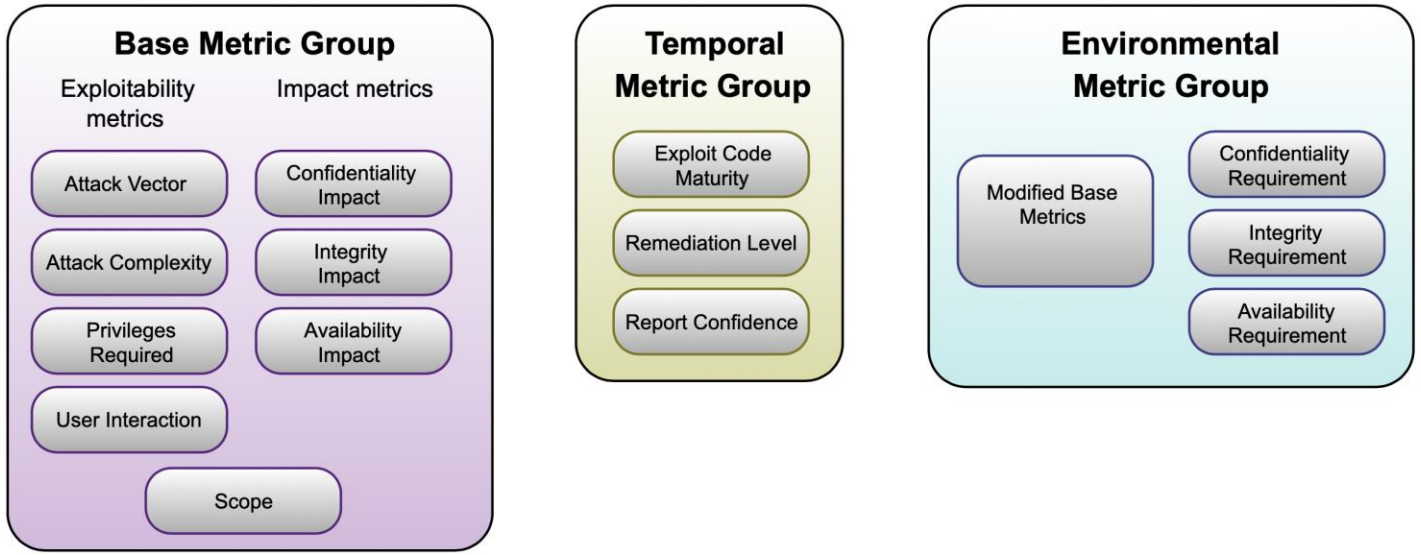
– Uma **metodologia para priorizar** vulnerabilidades com base nas necessidades das partes interessadas
  - Criada pelo CERT Division SEI/CMU em conjunto com a CISA
  - CISA instituiu um processo específico para o Governo dos EUA
  - **CISA** criou a base **KEV (*Known Exploited Vulnerabilities*)** como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

CVSS v3.1

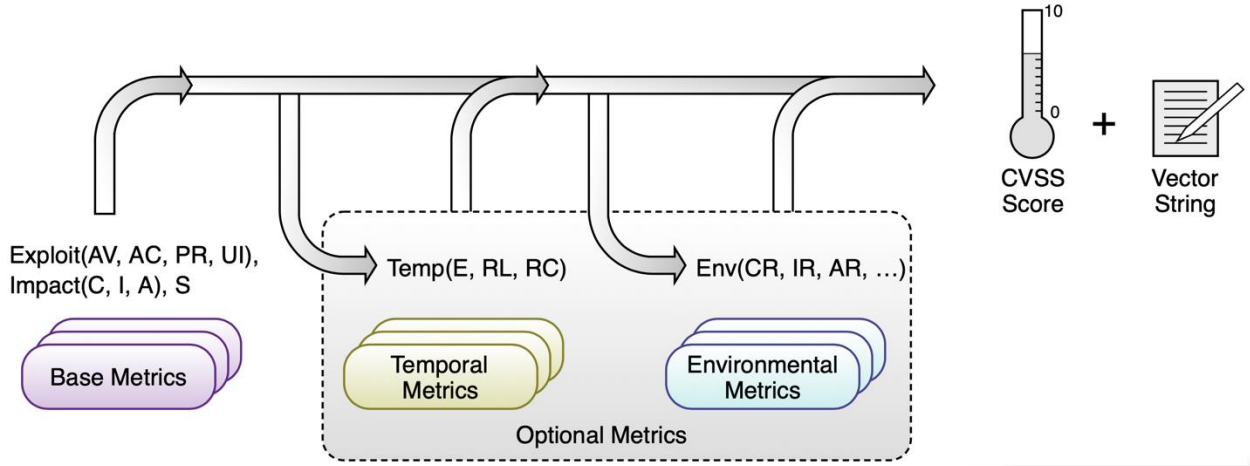
TLP:CLEAR

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

CVSS Metric Groups



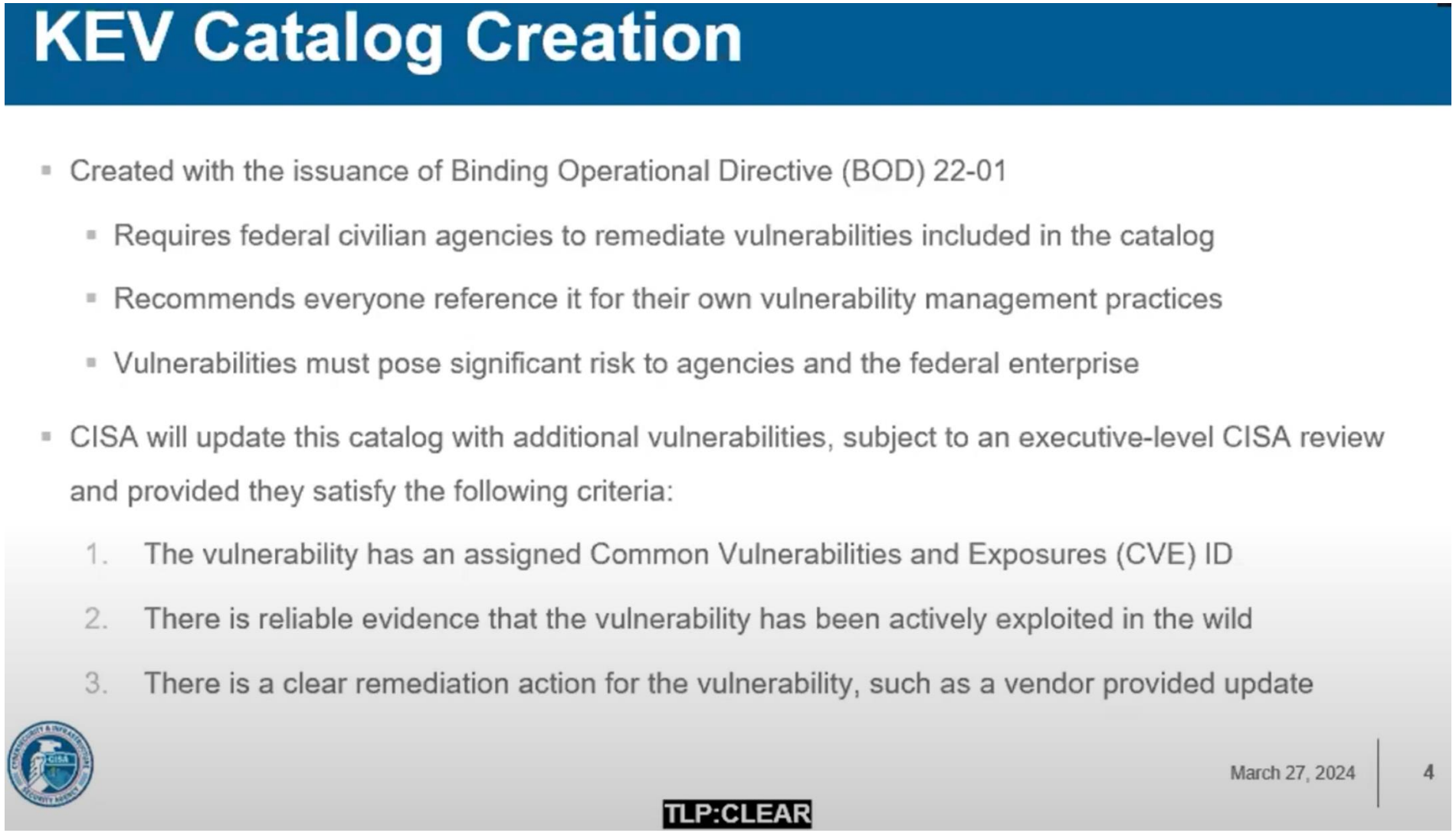
CVSS Metrics and Equations



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

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

EPSS
Exploit Prediction Scoring System

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."

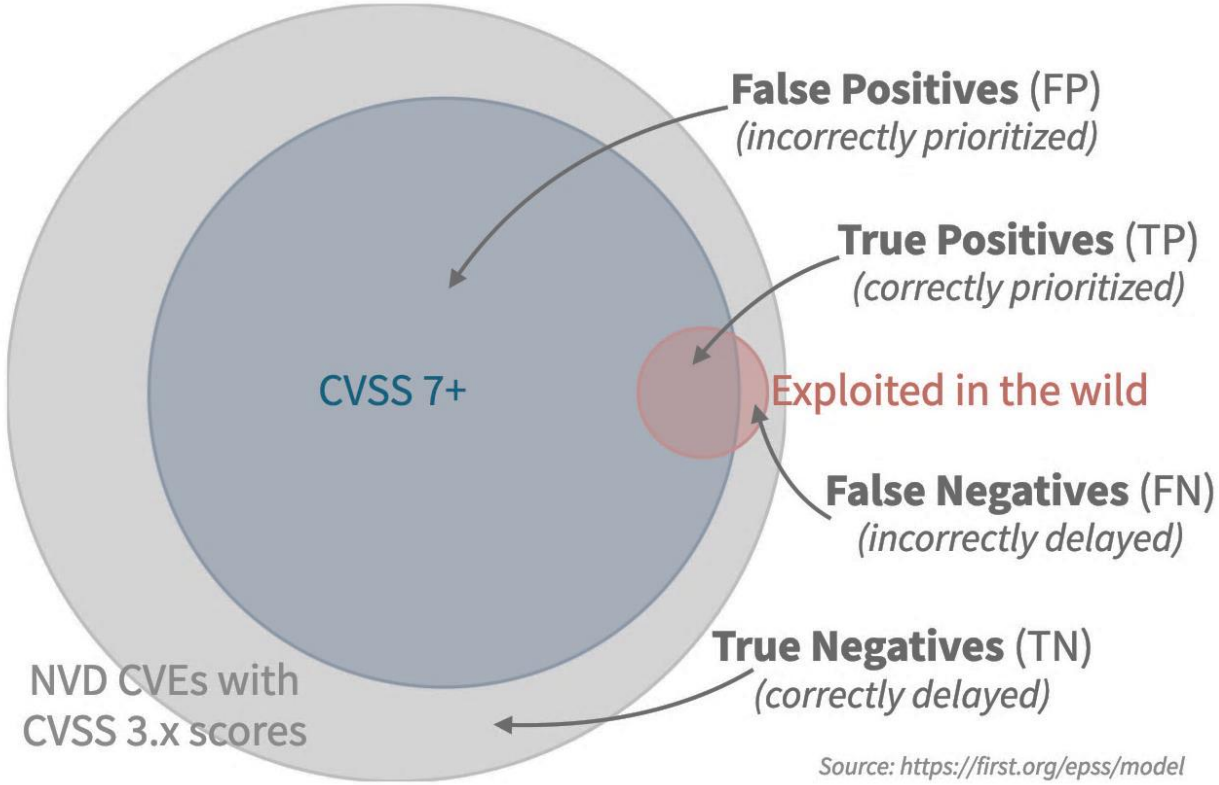
- Objetivo: ajudar as organizações a terem a melhor cobertura de aplicação de patches com o menor esforço (já que recursos são limitados)
- Dados levados em conta para o cálculo da pontuação: Idade do CVE, CPE, CWE, CVSS 3.x, CISA KEV, Google Project Zero, Trend Micro's Zero Day Initiative (ZDI), Exploit-DB, 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

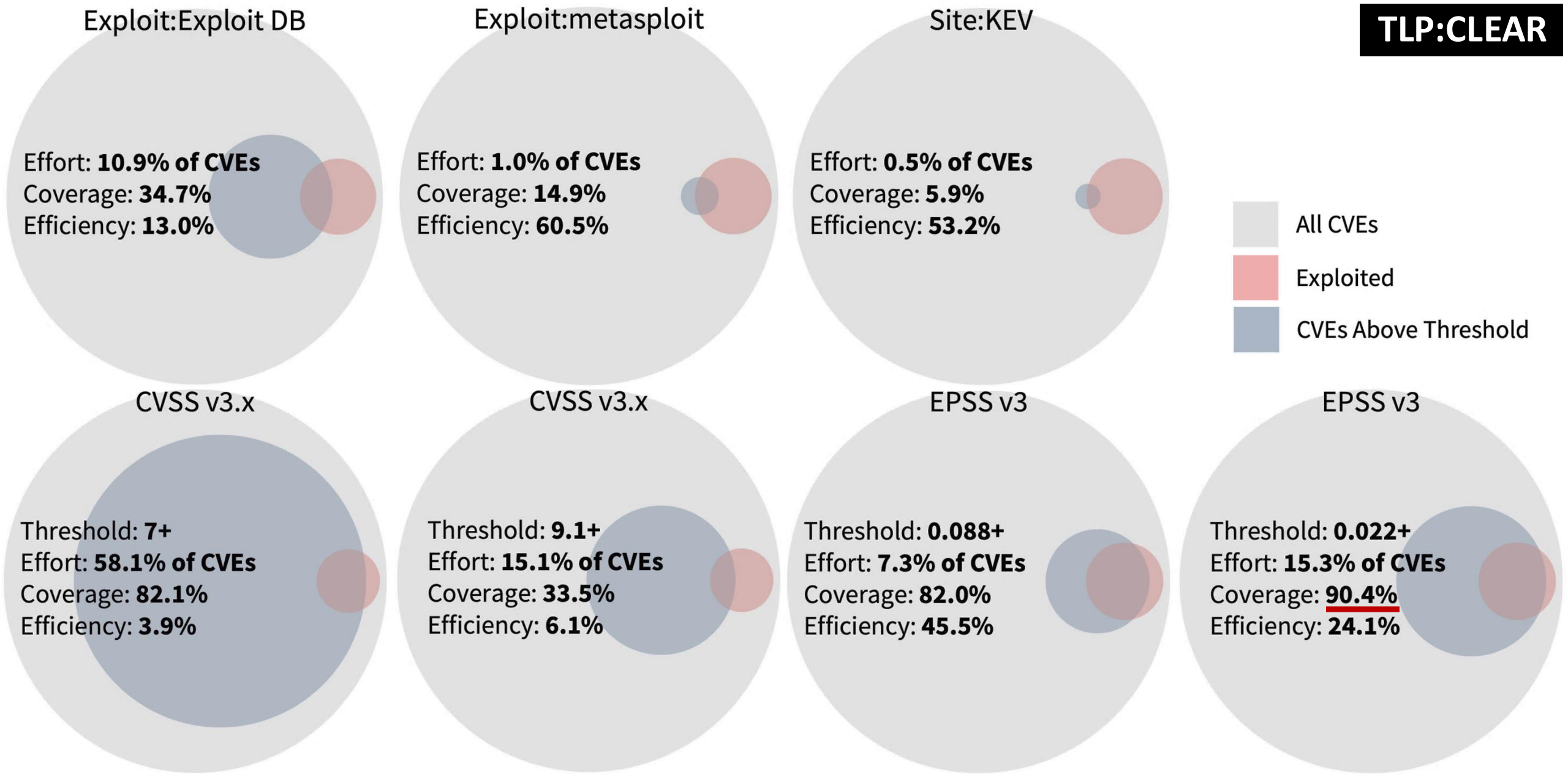
- 1 ano de dados usados para treinar o modelo
  - CVEs publicados entre 01/11/2021 – 31/10/2022
- Período de teste: dezembro/2022
- Avaliar para este mês
  - predições do EPSS versus
  - outras estratégias de priorização

Entendendo os Gráficos do próximo *slide*



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

TLP:CLEAR



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

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

TLP:CLEAR

- The European Union The Cyber Resilience Act
  https://www.cyberresilienceact.eu
- 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