



OWASP

TM

Priorização de Vulnerabilidades com Threat Intelligence

Frente a milhares de vulnerabilidades, quais representam o maior risco de exploração real?

Cristiano Henrique

Accenture - Application Security Specialist

OWASP Chapter Leader Fortaleza

Entusiasta de Tecnologias Open Source

Dev de Tools focadas em Security



Definições

#1 CVE

A sigla CVE – Common Vulnerabilities and Exposures, é uma lista de registro de ameaças e vulnerabilidades identificadas em softwares. Normalmente, ao se referir a CVE, a pessoa acaba indicando um número ID específico que cada registro na plataforma possui, organizando o catálogo.

Exemplo: CVE-2021-44228



#2 CVSS

O Common Vulnerability Scoring System (também conhecido como CVSS Scores) fornece uma representação numérica (0-10) da gravidade de uma vulnerabilidade de segurança da informação.



Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

#3 EPSS

O EPSS (Exploit Prediction Scoring System) que é um sistema que usa dados para estimar quão provável é que uma falha em um software seja explorada por ataques na internet, utilizando modelo de Machine Learning. Enquanto outros métodos avaliam a gravidade da falha, o EPSS vai além ao considerar informações em tempo real sobre ameaças e dados reais de ataques. Ele gera uma pontuação de probabilidade de 0 a 1, indicando quão alta é a chance de a falha ser explorada, sendo pontuações mais altas associadas a maior probabilidade de exploração.



#4 CISA

A CISA, ou Cybersecurity and Infrastructure Security Agency, é uma agência federal criada para liderar operacionalmente a cibersegurança federal e coordenar a segurança e resiliência da infraestrutura crítica nacional.



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

#5 KEV

O CISA KEV, ou Known Exploited Vulnerabilities Catalog, é um catálogo mantido pela Cybersecurity and Infrastructure Security Agency (CISA) que lista vulnerabilidades conhecidas que foram exploradas no ambiente digital. Esse catálogo é uma fonte autoritativa de vulnerabilidades exploradas na natureza, sendo essencial para a comunidade de cibersegurança e defensores de rede gerenciarem melhor as vulnerabilidades e acompanharem a atividade de ameaças.



Agrupando Conhecimentos

CVE

CISA

CVSS/EPSS

CISA KEV



Contexto Histórico

ATO 1: AGOSTO DE 2023 – ENTREGA

Em atendimento a um cliente, reportamos mais de 3000 mil vulnerabilidades encontradas nos softwares dele em um relatório detalhado e cheio de informações.



ATO 2: AGOSTO DE 2023 - QUESTIONAMENTO

O cliente retornou nossa entrega com o questionamento simples mas válido:

“Ótimo relatório, mas não tenho pessoas para corrigir tudo isso. Quais destas vulnerabilidades apresentam um risco real a minha empresa?”



ATO 3: SETEMBRO DE 2023 – COMO MELHORAR

Ao enfrentarmos este questionamento, buscamos informações de como priorizar uma vulnerabilidade baseada no risco real.

Ideias começaram a ser trocadas entre AppSec, Vulnerability Management e Threat Intelligence.



ATO 4: OUTUBRO DE 2023 – MELHORANDO...

Baseado no brainstorm gerado da interação das equipes, criamos um método de priorização de vulnerabilidades baseada em dados atuais e que realmente destaque o risco real.

Versão 0.1.0 do Intel-Toolkit



ATO 5: JANEIRO DE 2024 – MERCADO MUDOU

Após a criação da ferramenta, observamos por meio do LinkedIn uma movimentação do mercado de vulnerability management e utilizar os mesmos dados que nos.

**Lançamento do CVEMap com a
mesma visão do Intel-Toolkit**



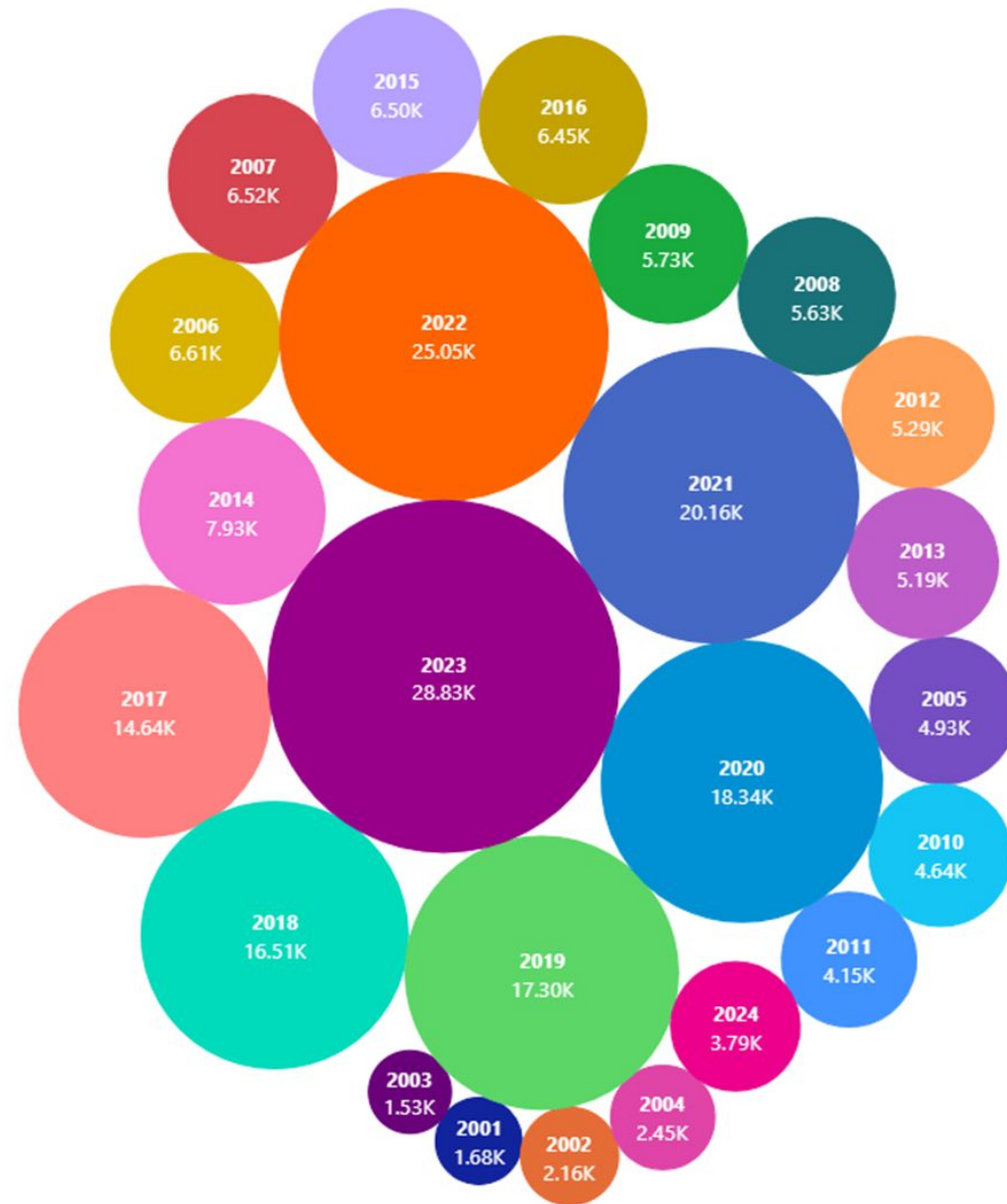
**Tá mas, qual o tamanho do problema, é
tão sério assim?!**

Milhares de Vulnerabilidades, Milhões de Problemas

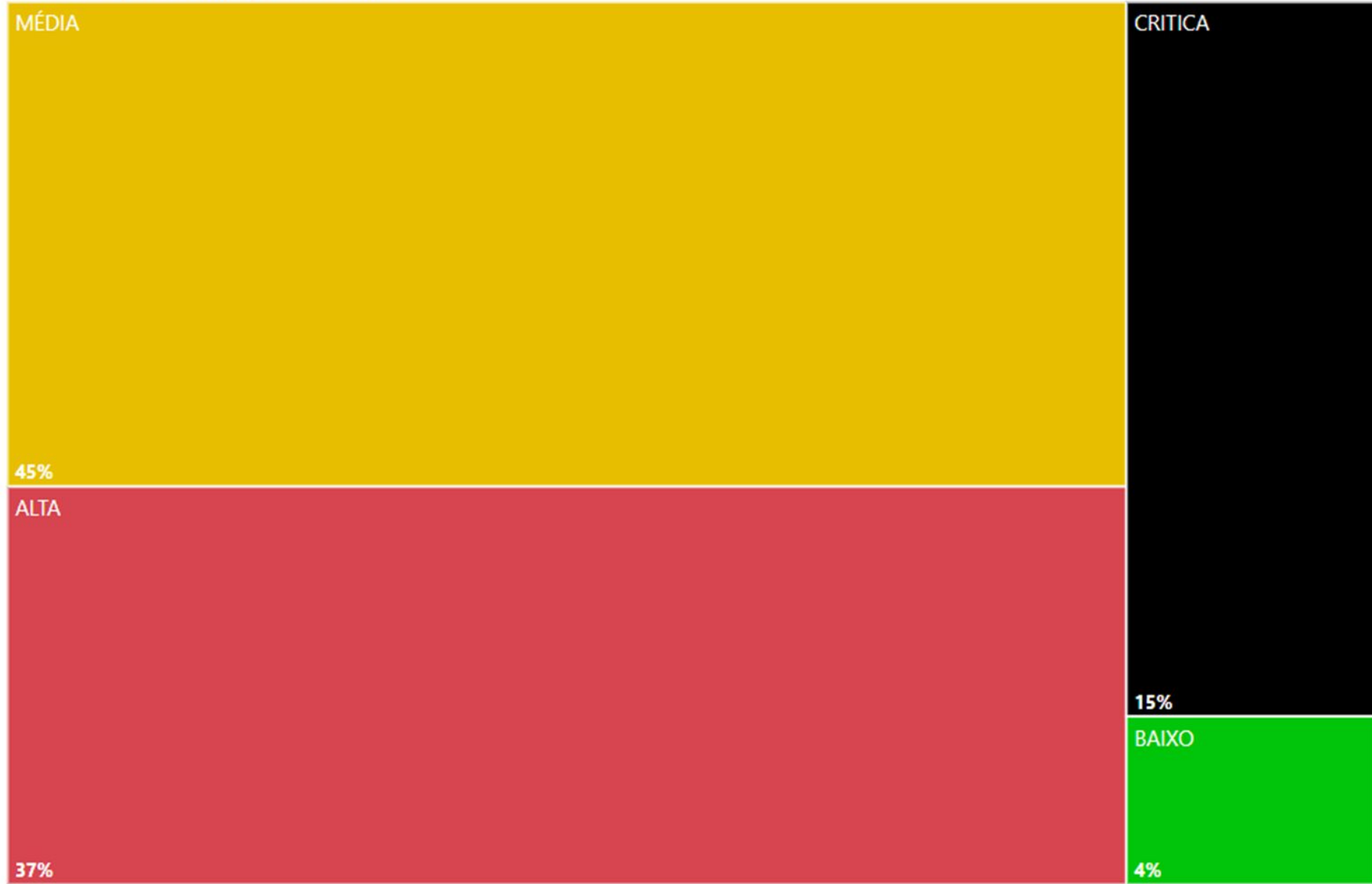
Quem é você no dia do Patch Tuesday?



Alguns dados que comprovam o problema crescente...

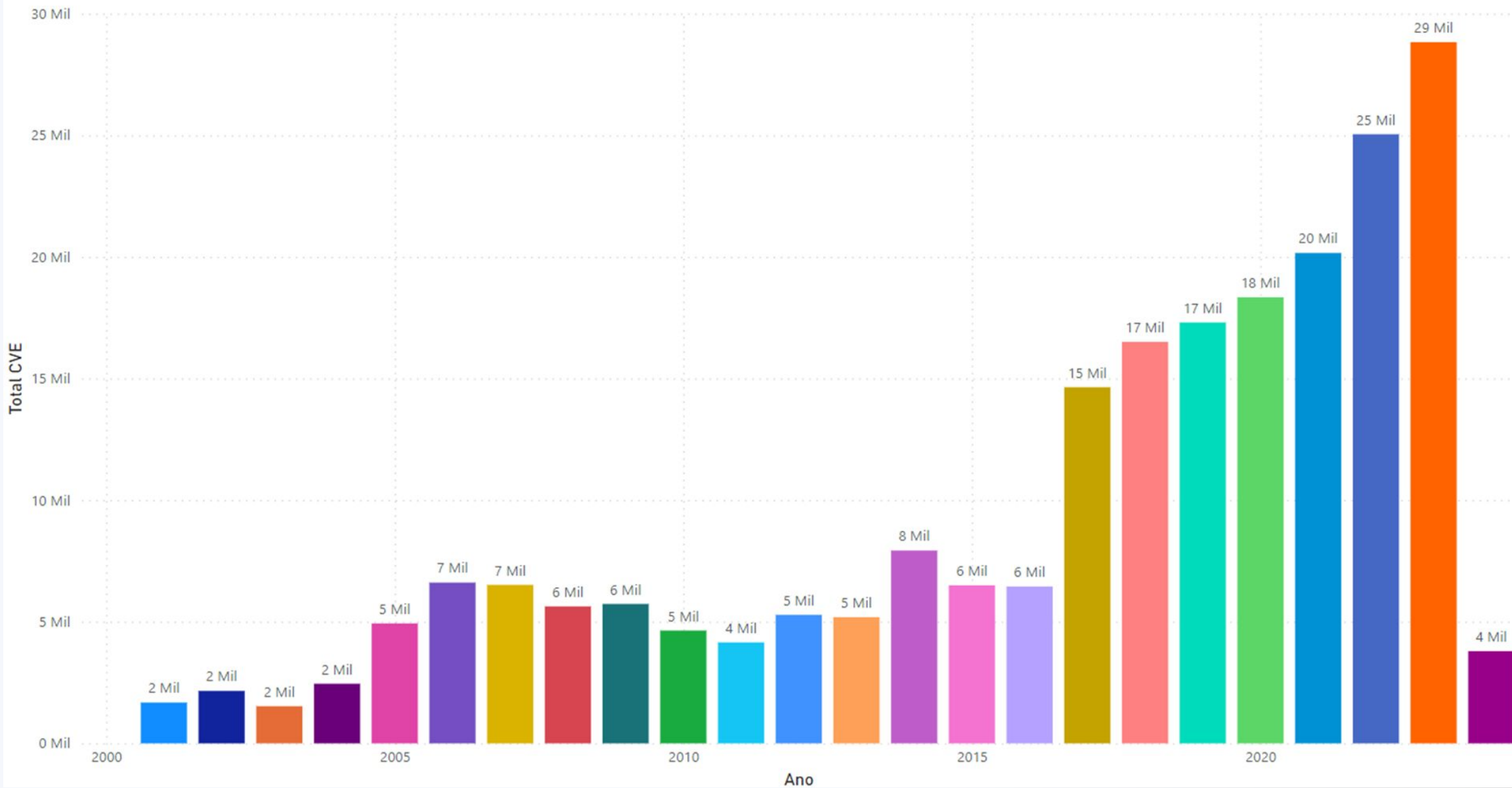


CVEs Proporcionais por Severidade



Comparativo de CVEs Ano a Ano

Ano ● 2001 ● 2002 ● 2003 ● 2004 ● 2005 ● 2006 ● 2007 ● 2008 ● 2009 ● 2010 ● 2011 ● 2012 ● 2013 ● 2014 ● 2015 ● 2016 ● 2017 ● 2018 ● 2019 ● 2020 ● 2021 ● 2022 ● 2023 ● 2024



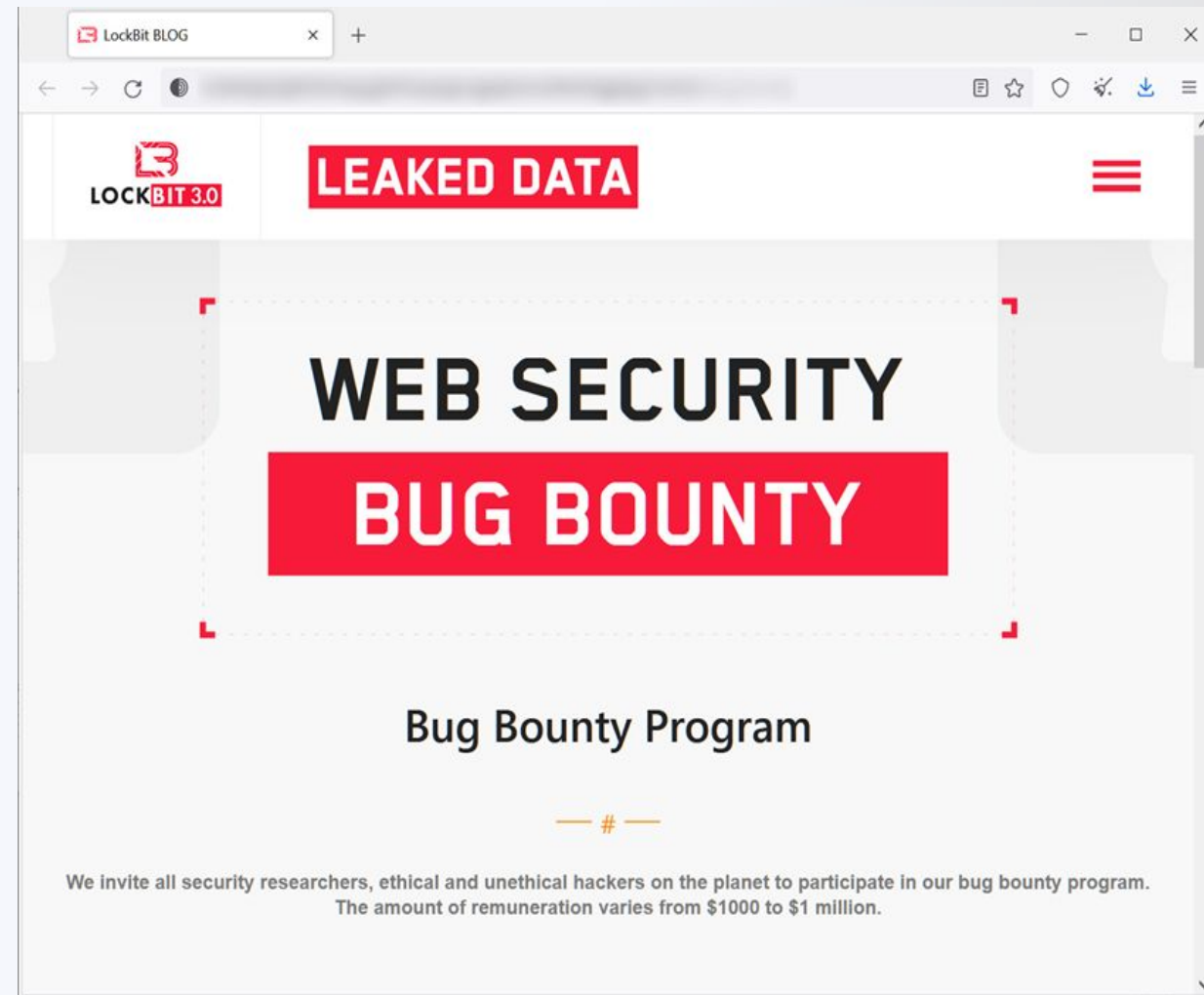
96~% de todas as vulnerabilidades reportadas desde 1999 tem um risco mapeado inicialmente como considerável...

Era do Raas



O que é RaaS?

Ransomware-as-a-service (RaaS) é um modelo de negócios para empresas criminosas que permite que qualquer pessoa se inscreva e use ferramentas para realizar ataques de ransomware. Como outros modelos como serviço, por exemplo, software como serviço (SaaS) ou plataforma como serviço (PaaS), os clientes de RaaS alugam serviços de ransomware, em vez de adquiri-los como em um modelo tradicional de distribuição de software.



Hackers embolsam recorde de US\$ 1 bi em criptos com ataques de ransomware

Montante registrado em 2023 é quase o dobro do de 2022, segundo a empresa de análise de dados em blockchain Chainalysis

[Lucas Gabriel Marins](#)

07/02/2024 17h00 • Atualizado 1 mês atrás



Pesquisa confirma que o ransomware ainda é o maior medo das empresas

Por Redação - 30 de outubro de 2023

0

👍 Curtir 2



A enquete *2023 SonicWall Threat Mindset*, que contou com a participação de quase 10.000 profissionais de tecnologia de todo o mundo, aponta que 55% estão mais preocupados com ataques cibernéticos em 2023. As principais ameaças são ataques digitais como *ransomware* e *spear phishing*. 83% do universo pesquisado afirma se angustiar com ataques com motivação financeira, enquanto 50% lutam para acompanhar a evolução do cenário de ameaças.

RANSOMWARE PELO MUNDO

O cibercrime como império seria a terceira maior economia do mundo



Brasiline



1 de setembro de 2022

O cibercrime custará ao mundo US\$ 10,5 trilhões anualmente até 2025

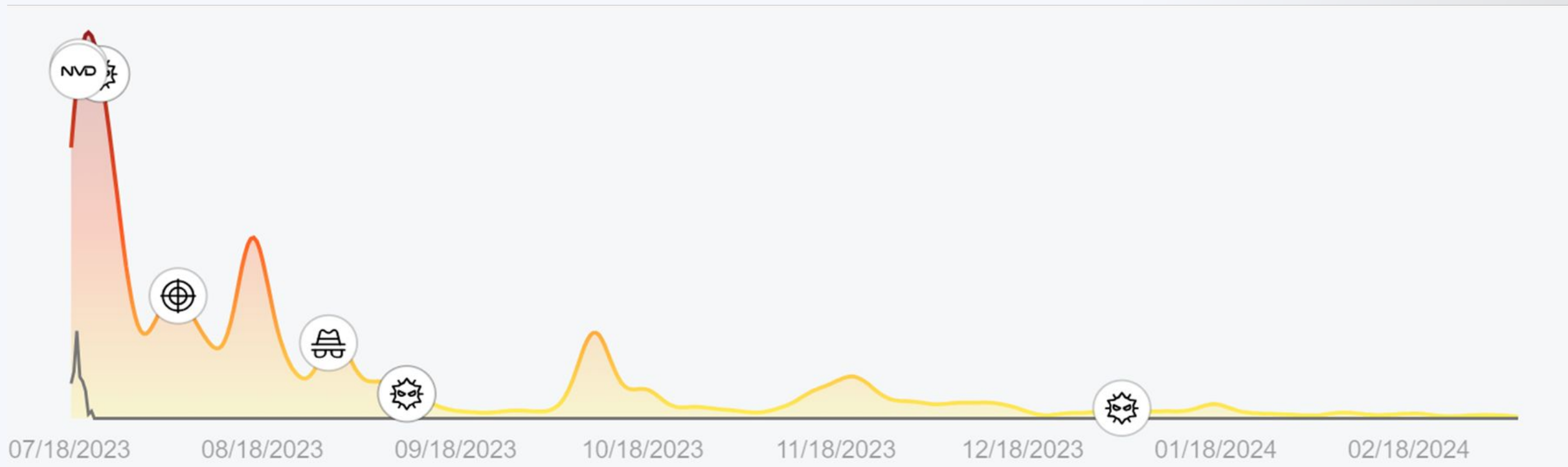
Se fosse medido como um país, o cibercrime – que infligiu danos totalizando 6 trilhões de dólares globalmente em 2021 – seria a terceira maior economia do mundo depois dos EUA e da China.

Ransomware é um preocupação de grandes corporações ainda hoje, está mais que provado.

Entendendo o ciclo de vida de uma vulnerabilidade



Citrix ADC/Gateway - CVE-2023-3519

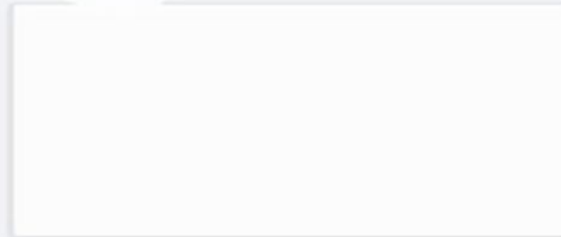


Citrix ADC/Gateway - CVE-2023-3519

Торговая площадка > MALWARE: вредоносы, крипт, инжекты, ... >

[Sell] Citrix 0day(RCE)

👤 ⏱ Jun 28, 2023



Пользователь

Joined: May 8, 2023
Messages: 3
Reaction score: -9

Jun 28, 2023

Spoiler: Closed for deposit

product: Citrix ADC management port.
version: 13.1 Build 48.47 is ok.
Contact with PM.

🔔 Report



CVE-2023-3519

Created: 07/19/2023
Last Update: 08/04/2023

CVSS 9.6

EPSS: 0.92538



7.5

Citrix ADC nsppe buffer overflow

2023-08-09



7.5

Citrix ADC (NetScaler) Remote Code Execution Exploit

2023-08-08



7.5

Exploit for Code Injection in Citrix Netscaler Application Delivery Controller

2023-08-05



7.5

Citrix ADC (NetScaler) Remote Code Execution

2023-08-04




7.5

Citrix ADC (NetScaler) Forms SSO Target RCE

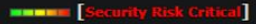
2023-07-31

Citrix ADC/Gateway - CVE-2023-3519

[Contact us](#) [\[authorization \]](#) [\[registration \]](#) [\[restore account \]](#)

 0DAY.today?

Citrix ADC (NetScaler) Remote Code Execution Exploit
[0Day-ID-38953]

Full title	Citrix ADC (NetScaler) Remote Code Execution Exploit [Highlight]
Date add	08-08-2023
Category	remote exploits
Platform	unix
Verified	✓
Price	free
Risk	 [Security Risk Critical]
Rel. releases	R
Description	A vulnerability exists within Citrix ADC that allows an unauthenticated attacker to trigger a stack buffer overflow of the nsppc process by making a specially crafted HTTP GET request. Successful exploitation results in remote code execution as root.
CVE	CVE-2023-3519
Abuses	0
Comments	0
Views	3 099

[We DO NOT use Telegram or any messengers / social networks! Please, beware of scammers!](#)

[Comments: 0]

free

[Open Exploit](#)

✓ Verified by 0day Admin

Author **metasploit**

BL 29

Exploits 1612

Readers 57



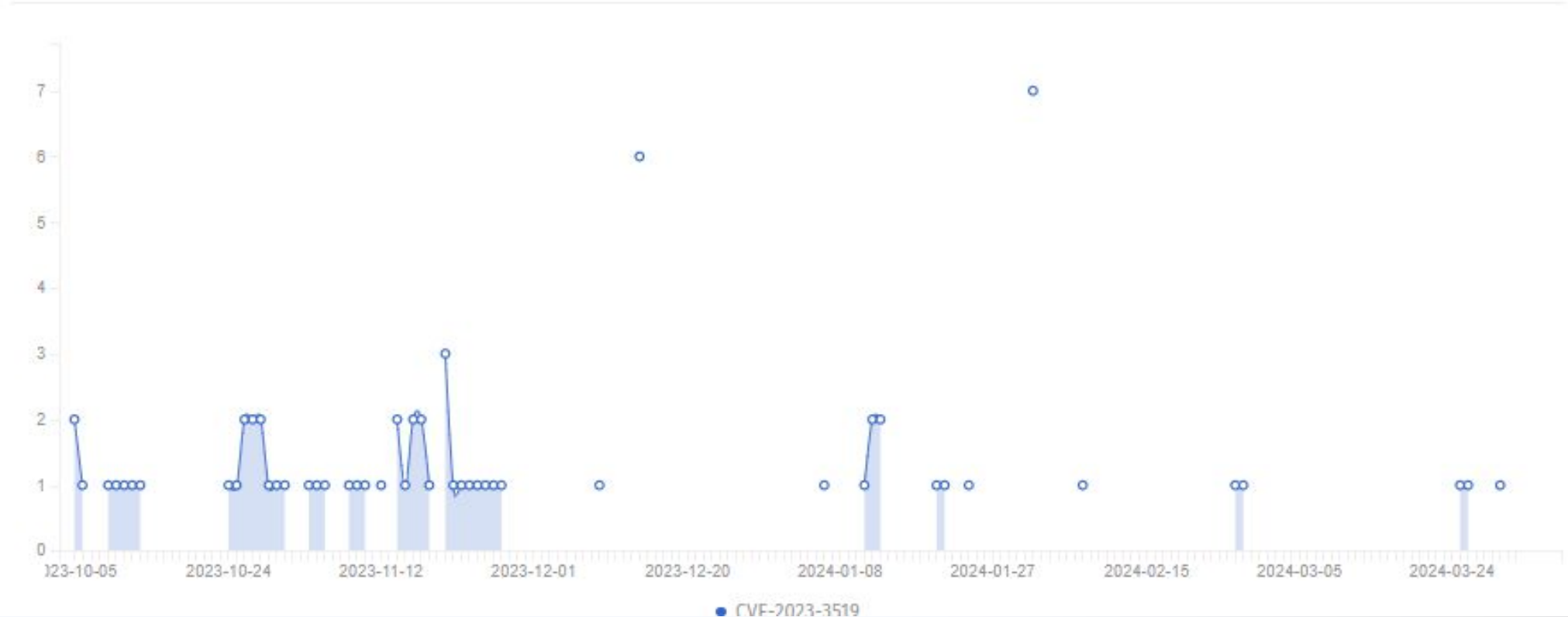
Created: 07/19/2023
Last Update: 08/04/2023

CVE-2023-3519 - Honeyypots

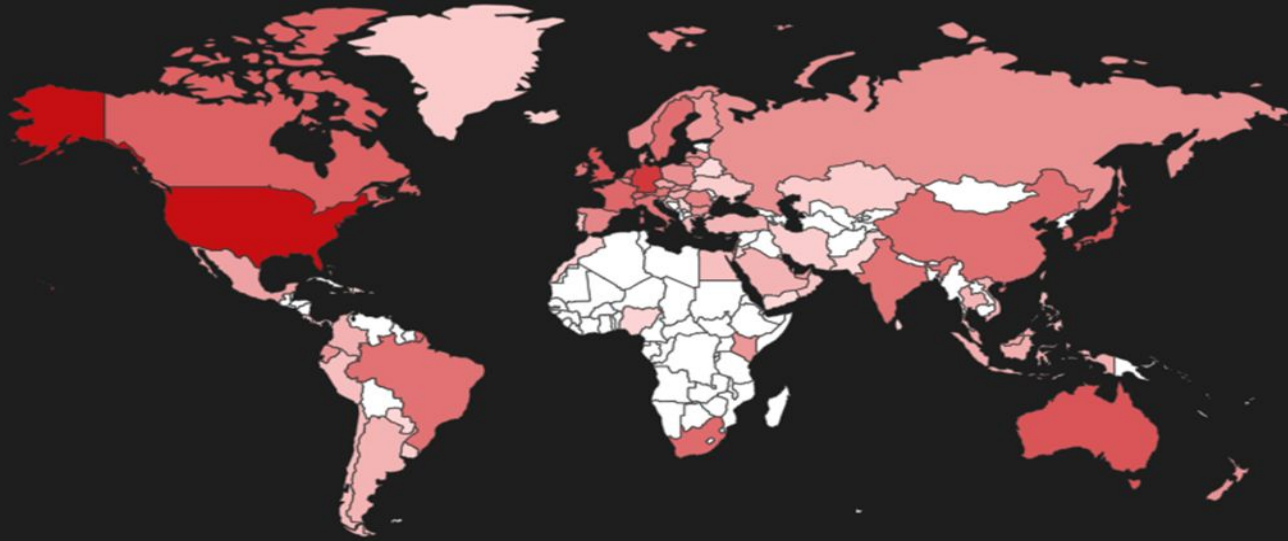
CVSS 9.6

EPSS: 0.92538

Results



// GENERAL



🌐 Countries

United States	22,700
Germany	9,030
United Kingdom	4,538
Japan	4,417
Australia	4,327

🏗️ Ports

443	50,741
9443	524
444	474
8443	447
4443	273

MORE...

🏢 Organization

Amazon Technologies Inc.	3,280
Microsoft Corporation	2,524
Amazon.com, Inc.	2,181
A100 ROW GmbH	1,191
Amazon Data Services UK	1,082

MORE...

⚠️ Vulnerabilities

FREAK	98
Logjam	12



CVE-2023-3519 - Honeyd

CVSS 9.6

EPSS: 0.92538



Malwares

- Conti
- Clop



Threat Actors

- FIN8
- johndoe7
- APT5



TTPs

- T1087
- T1087.002
- T1016
- T1505.003
- T1090
- T1046
- T1562
- T1552...



Created: 07/19/2023
Last Update: 08/04/2023

CVE-2023-3519 - Honeyypots

CVSS 9.6

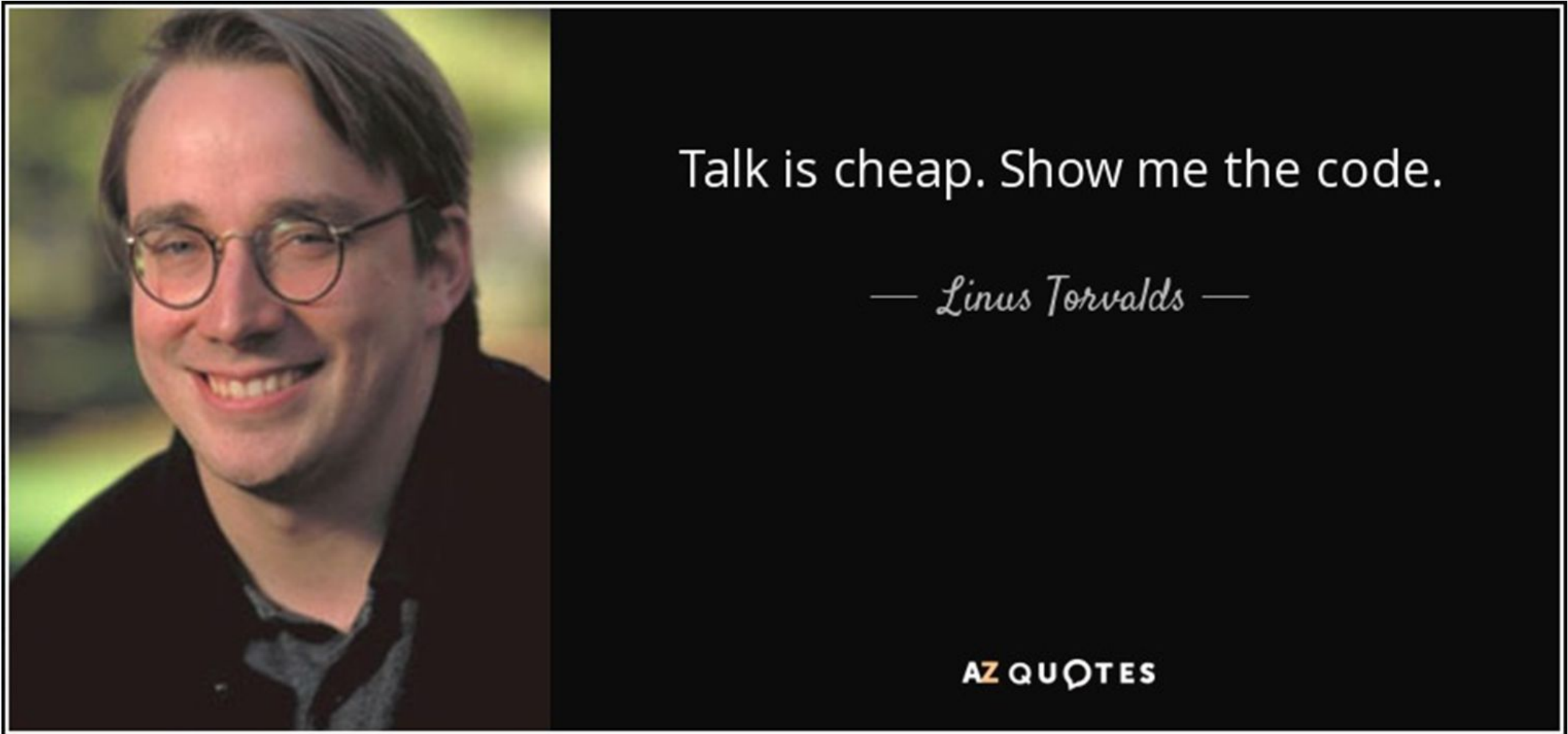
EPSS: 0.92538

Citrix CVE



Tu já falou de mais como é que faz isso?

Vamos para a prática...



CVE Risk-Based Patch Prioritization

Row ID	Priority	Severity	CVE	CVSS	EPSS	HoneyPot	Status	Interest Status	Exploitation Status	Mitigation Status	Ransomware Campaign	CVE Trends	Has Nuclei Template	OWASP TOP 10
1	Priority 1++	CRITICAL	CVE-2024-1709	10.0	0.93461	🔥 3884 Attacks	Analyzed	🔴 Exploited	🟡 Productized	🛑 Available	🔒 In use	📉 Audience 572344	🟢 Finded	A07:2021 - Identification and Authentication Failures A01:2021 - Broken Access Control A03:2021 - Injection A03:2021 - Injection
2	Priority 1++	HIGH	CVE-2020-3259	7.5	0.01928	-	Analyzed	🔴 Exploited	🟡 Unobserved	🛑 Available	🔒 In use	📉 Audience 940167	🔴 Not finded	
3	Priority 1++	CRITICAL	CVE-2022-26134	9.8	0.9753	🔥 7088 Attacks	Modified	🔴 Exploited	🟡 Productized	🛑 Available	🔒 In use	-	🟢 Finded	
4	Priority 1++	CRITICAL	CVE-2023-22527	9.8	0.96568	🔥 5689 Attacks	Modified	🔴 Exploited	🛑 Code Available	🛑 Available	🔒 In use	📉 Audience 87826	🟢 Finded	
5	Priority 1+	HIGH	CVE-2022-4262	8.8	0.0052	-	Analyzed	🔴 Exploited	🛑 Code Available	🛑 Available	🔒 Not in use	-	🔴 Not finded	
6	Priority 1+	HIGH	CVE-2023-26369	7.8	0.0413	-	Analyzed	🔴 Exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	-	🔴 Not finded	
7	Priority 1+	HIGH	CVE-2023-29360	8.4	0.00409	-	Analyzed	🔵 Not exploited	🛑 Code Available	🛑 Available	🔒 Not in use	-	🔴 Not finded	
8	Priority 1+	HIGH	CVE-2024-21338	7.8	0.00079	-	Modified	🔴 Exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	📉 Audience 173003	🔴 Not finded	
9	Priority 1+	CRITICAL	CVE-2024-21410	9.8	0.02321	-	Analyzed	🔴 Exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	-	🔴 Not finded	
10	Priority 1+	HIGH	CVE-2024-21412	8.1	0.00316	-	Analyzed	🔴 Exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	📉 Audience 291914	🔴 Not finded	
11	Priority 1+	CRITICAL	CVE-2024-21762	9.8	0.02287	-	Analyzed	🔴 Exploited	🟡 Productized	🛑 Available	🔒 Not in use	📉 Audience 355166	🔴 Not finded	
12	Priority 1+	HIGH	CVE-2024-21893	8.2	0.96249	🔥 825 Attacks	Analyzed	🔴 Exploited	🟡 Productized	🛑 Available	🔒 Not in use	-	🟢 Finded	
13	Priority 1+	HIGH	CVE-2024-23225	7.8	0.00127	-	Modified	🔵 Not exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	-	🔴 Not finded	
14	Priority 1+	CRITICAL	CVE-2024-27198	9.8	0.97174	🔥 6218 Attacks	Modified	🔵 Not exploited	🟡 Productized	🛑 Available	🔒 Not in use	📉 Audience 213694	🟢 Finded	
15	Priority 1	HIGH	CVE-2021-43798	7.5	0.97474	🔥 13 Attacks	Analyzed	🔵 Not exploited	🟡 Productized	🛑 Available	🔒 Not in use	-	🟢 Finded	
16	Priority 2	MEDIUM	CVE-2014-4078	5.1	0.00817	-	Modified	🔵 Not exploited	🟡 Unobserved	💀 Unavailable	🔒 Not in use	-	🔴 Not finded	
17	Priority 2	LOW	CVE-2019-19534	2.4	0.00321	-	Analyzed	🔵 Not exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	-	🔴 Not finded	
18	Priority 2	CRITICAL	CVE-2022-27255	9.8	0.07698	-	Analyzed	🔵 Not exploited	🛑 Code Available	🛑 Available	🔒 Not in use	-	🔴 Not finded	
19	Priority 2	HIGH	CVE-2023-21746	7.8	0.00043	-	Modified	🔵 Not exploited	🛑 Code Available	💀 Unavailable	🔒 Not in use	📉 Audience 152326	🔴 Not finded	
20	Priority 2	HIGH	CVE-2023-21987	7.8	0.00091	-	Analyzed	🔵 Not exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	📉 Audience 161864	🔴 Not finded	
21	Priority 2	CRITICAL	CVE-2023-28578	9.3	0.00053	-	Awaiting Analysis	🔵 Not exploited	🟡 Unobserved	💀 Unavailable	🔒 Not in use	-	🔴 Not finded	
22	Priority 2	CRITICAL	CVE-2023-36049	9.8	0.00099	-	Analyzed	🔵 Not exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	-	🔴 Not finded	
23	Priority 2	MEDIUM	CVE-2023-41703	6.1	0.00043	-	Awaiting Analysis	🔵 Not exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	-	🔴 Not finded	
24	Priority 2	HIGH	CVE-2023-42902	7.8	0.00092	-	Analyzed	🔵 Not exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	-	🔴 Not finded	
25	Priority 2	CRITICAL	CVE-2023-48788	9.8	0.00043	-	Analyzed	🔵 Not exploited	🟡 Unobserved	💀 Unavailable	🔒 Not in use	📉 Audience 87683	🔴 Not finded	
26	Priority 2	MEDIUM	CVE-2023-4969	6.5	0.00065	-	Analyzed	🔵 Not exploited	🟡 Unobserved	🛑 Available	🔒 Not in use	📉 Audience 151039	🔴 Not finded	
27	Priority 2	CRITICAL	CVE-2023-49785	9.1	0.00049	-	Awaiting Analysis	🔵 Not exploited	🟡 Unobserved	💀 Unavailable	🔒 Not in use	📉 Audience 113852	🟢 Finded	
28	Priority 2	CRITICAL	CVE-2023-50164	9.8	0.09719	-	Analyzed	🔴 Exploited	🛑 Code Available	🛑 Available	🔒 Not in use	-	🔴 Not finded	

Futuro:

Tornar a ferramenta 100% offline

Mapeamento de TTPs do Mitre Att&ck e correlacionar ao Mitre D3fende



OWASP

TM

OBRIGADO!