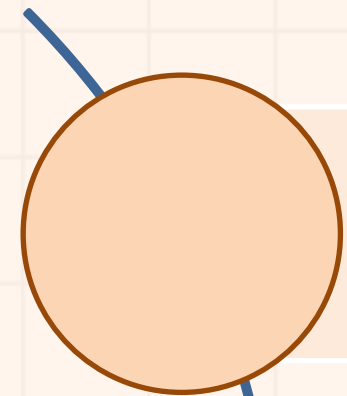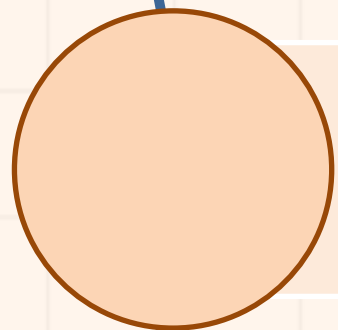# Porto Business School

19/05/2025
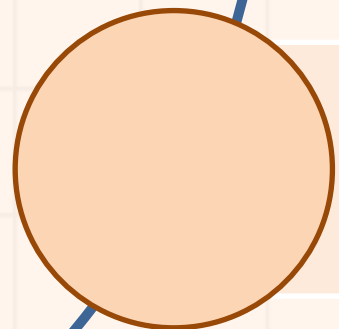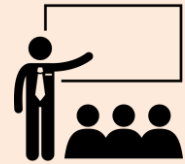
Agenda

Vulnerability

Common Attack Vectors

Portuguese landscape

Disclaimer & Legal Considerations

Presentation is solely for educational and awareness purposes.

Live content may be unpredictable and potentially inappropriate for some viewers.

Users must check the legality of OSINT tools and methods in their country.

This presentation is <u>not related</u> to my work or employer.

images: Flaticon.com

Disclaimer & Legal Considerations

- **Portuguese Law**
  - Diário República Eletrónico (link)
  - ANACOM (link)
- **Organizations**
  - CNCS – Centro Nacional de Cibersegurança (link)
    - Incident Notification (link)
    - CERT.PT (link)
  - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) (link)
  - Ministério Público (link)
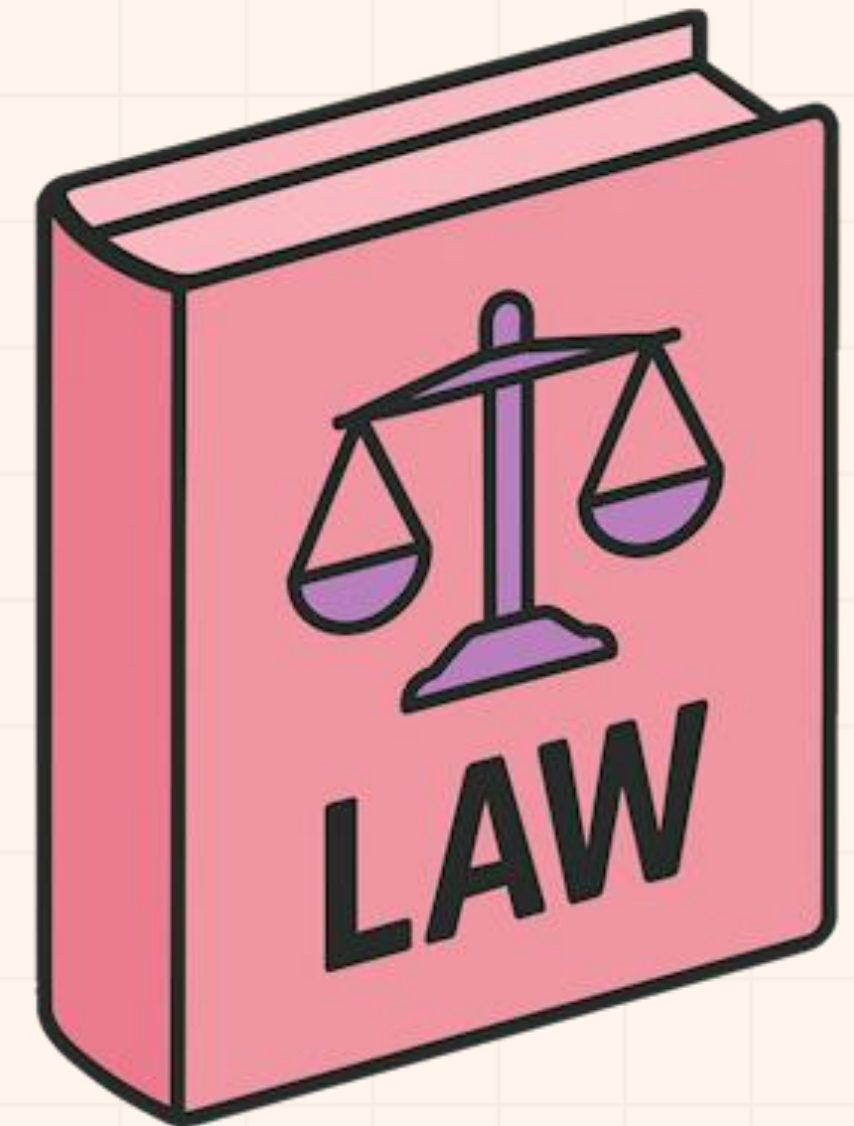
$whoami

🕶️ Pedro Vieira

🔐 Cybersecurity Engineer

🕵️ OSINT

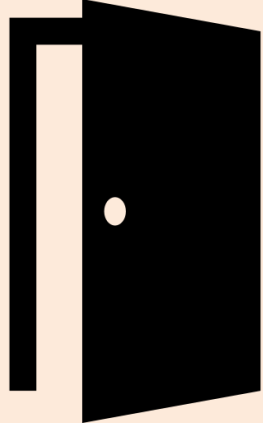🖊️ Full stack developer

👨‍🏫 Public Speaker

Vulnerability

Definition and Statistics

Vulnerability - Vulnerability vs incident

Logged In Remote Access
"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability."
National Vulnerability Database - https://nvd.nist.gov/vuln

Vulnerability	Incident
Open door	Unauthorized access

images: Flaticon.com   **Page 7**

Vulnerability - Statistics by Year
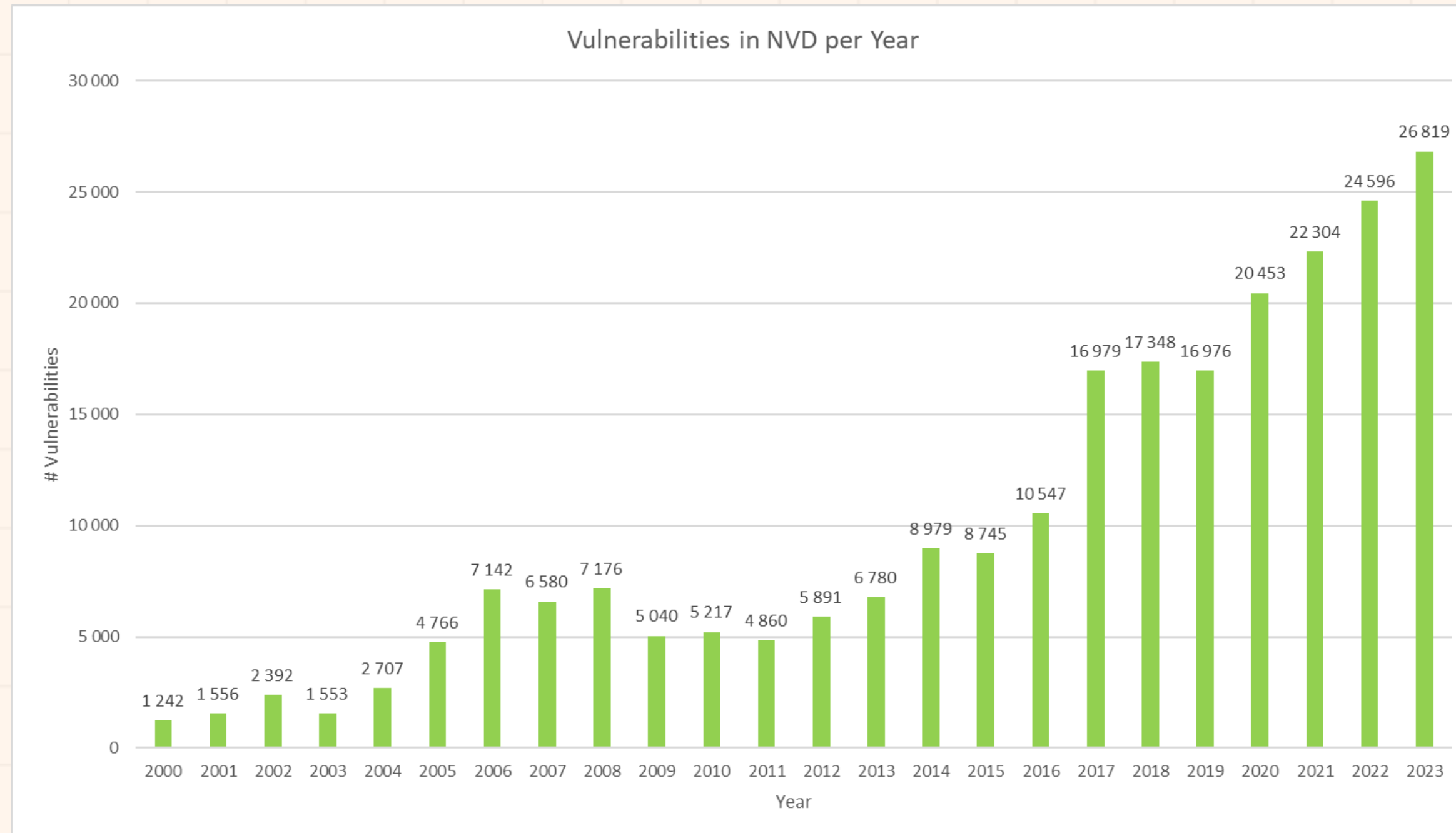
Total known vulnerabilities

283.154

Source NVD 14/03/2024

Vulnerability - Statistics by Severity

Vulnerabilities in NVD by Severity
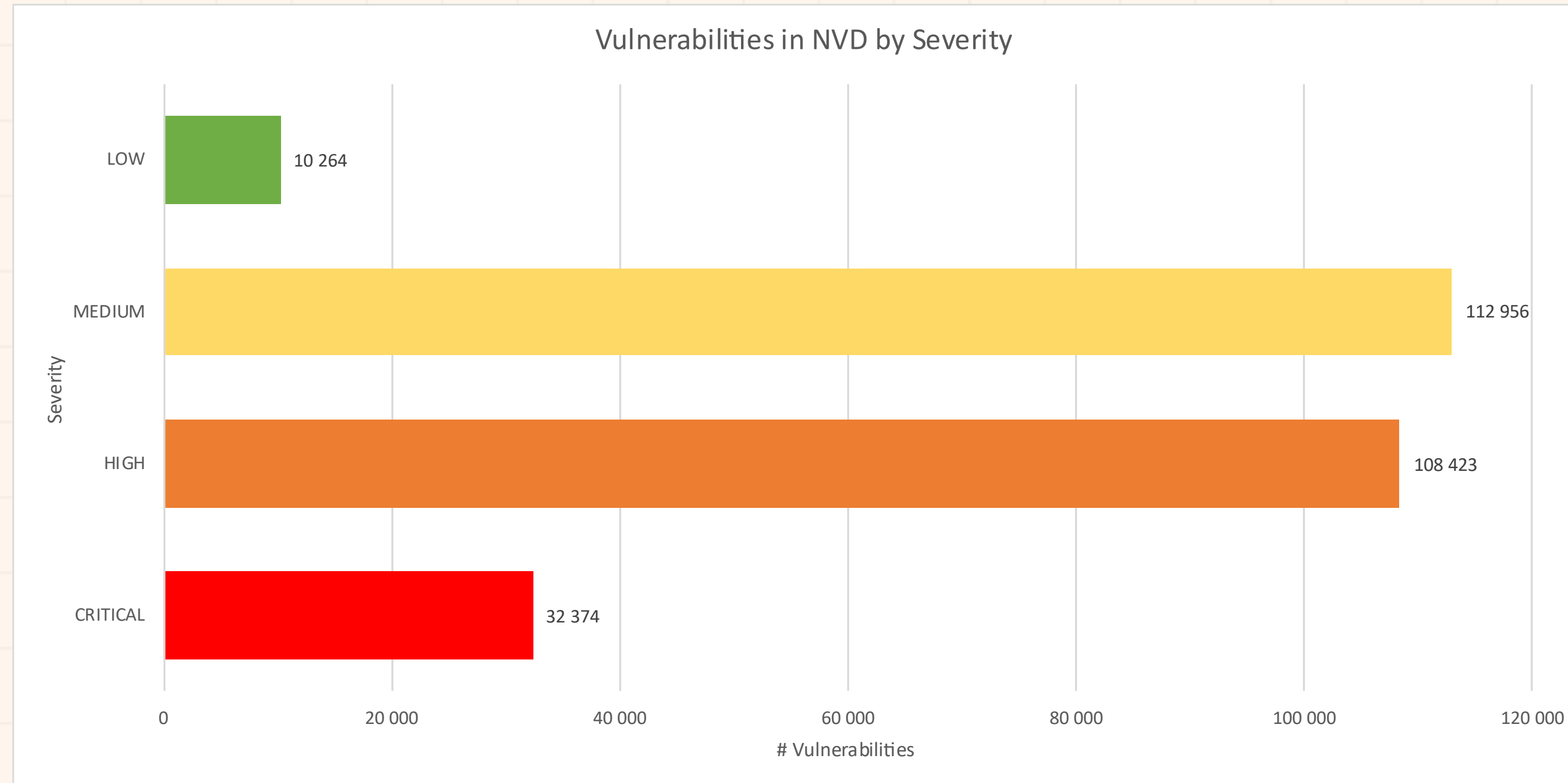
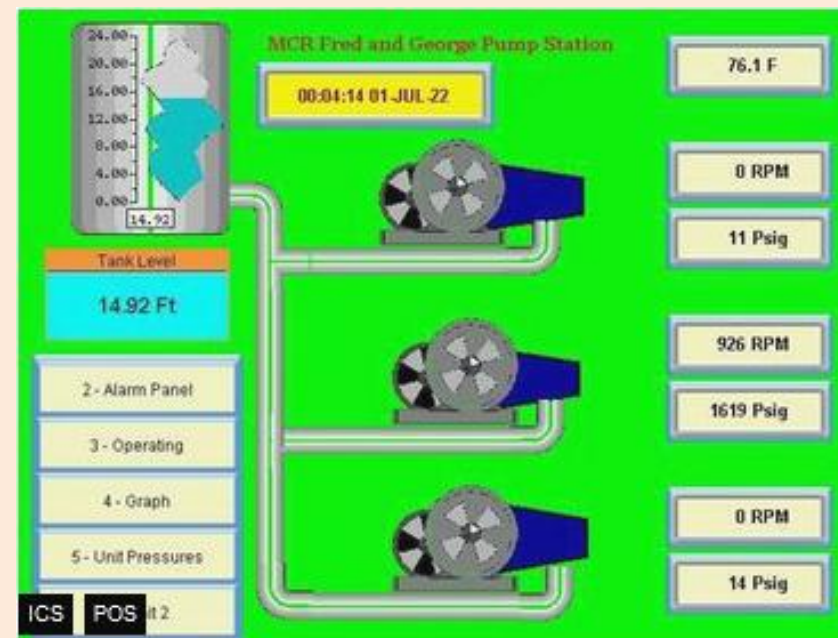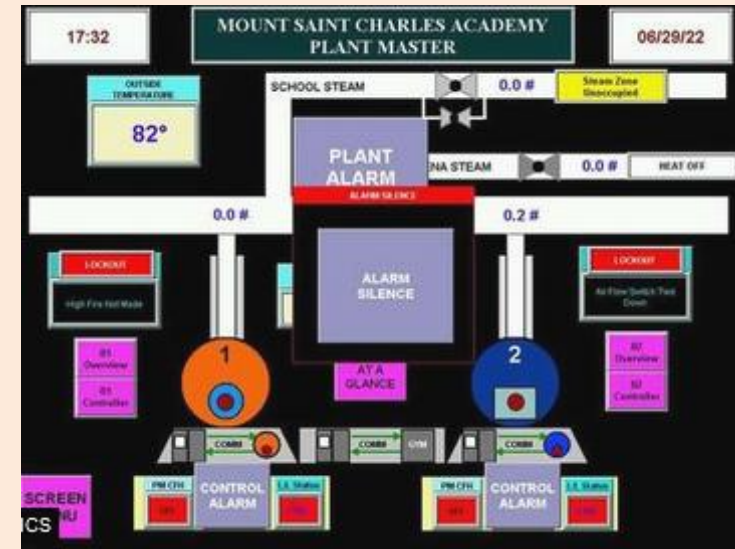| CVSS v3.1 Ratings	
LOW	0.1 - 3.9
MEDIUM	4.0 - 6.9
HIGH	7.0 - 8.9
CRITICAL	9.0 - 10.0

Source NVD 14/03/2024

Vulnerability - Examples from Shodan.io

Default/No Password	Industrial Control Systems	Vulnerable Systems
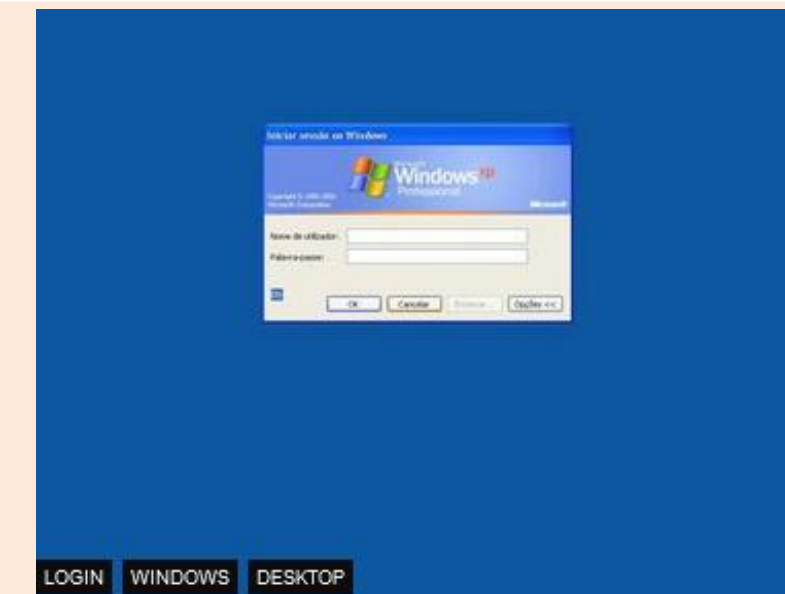
Common Attack Vectors

Easy-Peasy

Common Attack Vectors - Credentials

Insecure	Compromised/Leaked
• No password • Default credentials (admin/admin) • Weak passwords • Reused passwords	• Hacked legitime sites leaked user information and credentials • Mother of all breaches reveals 26 billion records

Common Attack Vectors - Misconfiguration

Shared Folder – Authentication disabled

WordPress site – Configuration available

Common Attack Vectors - Software Vulnerabilities

Shared Folder - Remote Code Execution	Website – Several vulnerabilities

Common Attack Vectors - Malware - Ransomware

Redeemer Ransomware	Ransomwatch

Portugal - Shodan.io - Search Engine for Internet Of Things

Ransomwatch	NoMoreRansom

Portuguese landscape

Definition and Statistics

Portugal - Shodan.io - Search Engine for Internet Of Things

Explore	Images

Shodan Queries (link)

Portugal - Shodan.io - Search Engine for Internet Of Things

Internet Exposure Observatory
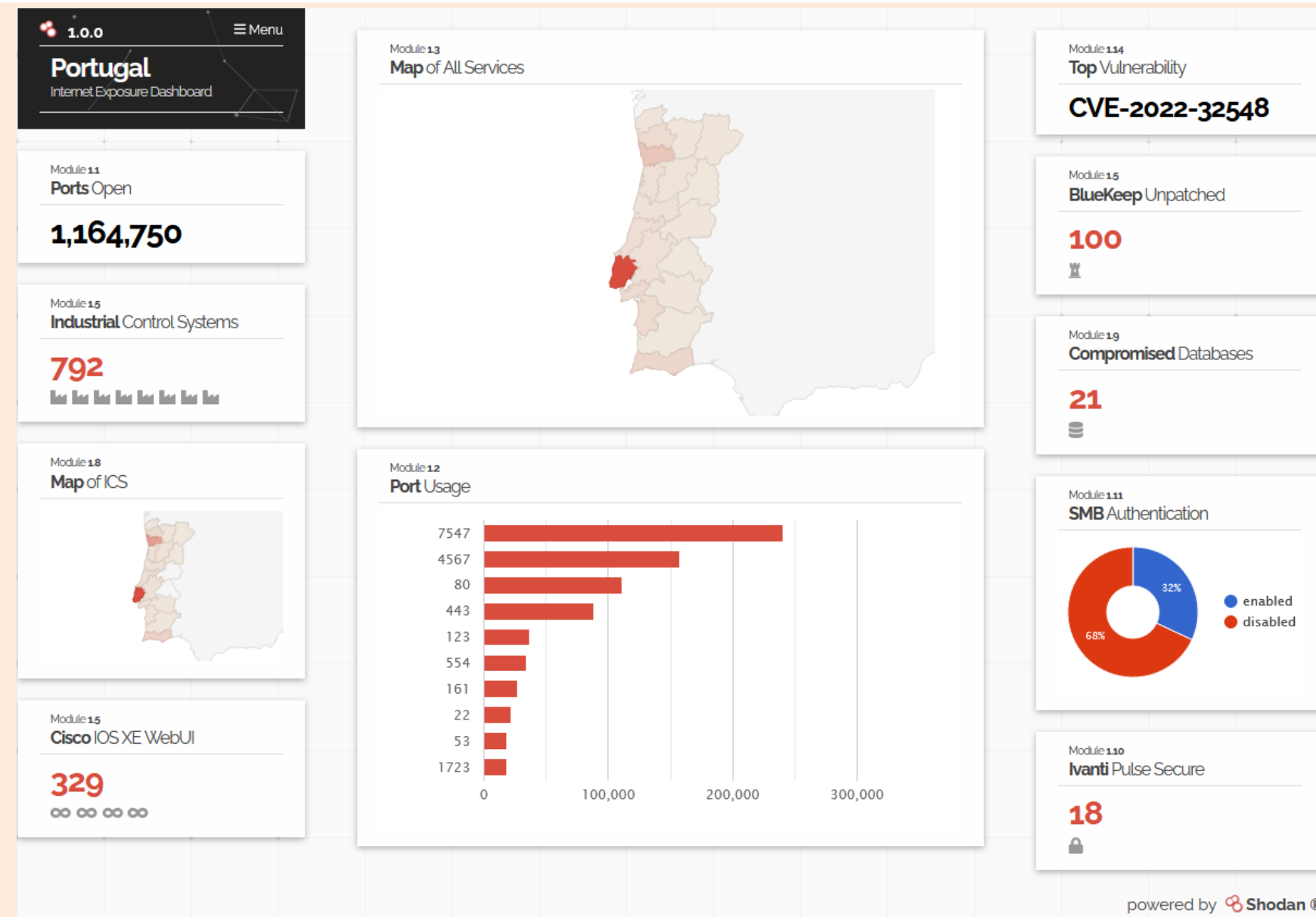
Portugal - Shodan.io - Search Engine for Internet Of Things

Top in Portugal - CVE-2022-32548	EternalBlue - MS17-010 - CVE-2017-0144

⚠ **Vulnerabilities**

CVE-2022-32548   **10.0**   Unauthenticated Remote Code Execution in a Wide Range of DrayTek Vigor Routers

TOTAL RESULTS

3,322

TOP CITIES

Lisbon	991
Leiria	181
Porto	114
Braga	95
Rio Maior	83

More...

⚠ **Vulnerabilities**

MS17-010   **8.1**   This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. This security update is rated Critical for all supported releases of Microsoft Windows.

TOTAL RESULTS

6

TOP CITIES

Lisbon	2
Braga	1
Porto	1
Silves	1
Évora	1

More...

Portugal - Shodan.io - Search Engine for Internet Of Things

Heartbleed - CVE-2014-0160	SMBGhost - CVE-2020-0796

⚠ **Vulnerabilities**

CVE-2014-0160 **5.0** The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

TOTAL RESULTS

311

TOP CITIES

Lisbon	146
Coimbra	20
Porto	12
Rio Maior	8
Torres Vedras	7
More...	

⚠ **Vulnerabilities**

CVE-2020-0796 **10.0** A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server or client.

TOTAL RESULTS

554

TOP CITIES

Lisbon	263
Porto	29
Braga	13
Guimarães	8
Montijo	8
More...	

Portugal - Shodan.io - Search Engine for Internet Of Things

BlueKeep - CVE-2019-0708
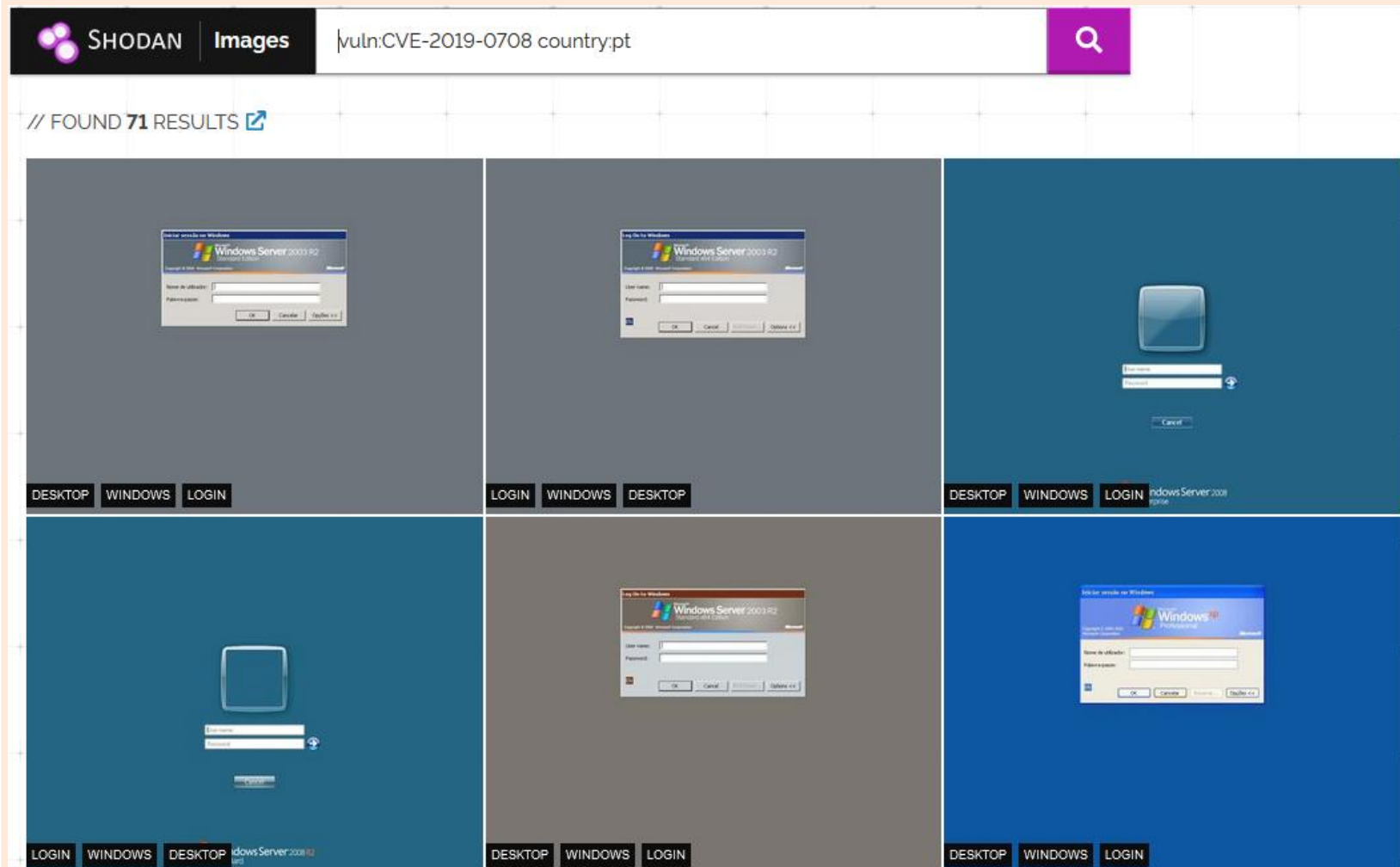
Portugal - Shodan.io - Search Engine for Internet Of Things

Shared Folders

Portugal - Shodan.io - Search Engine for Internet Of Things
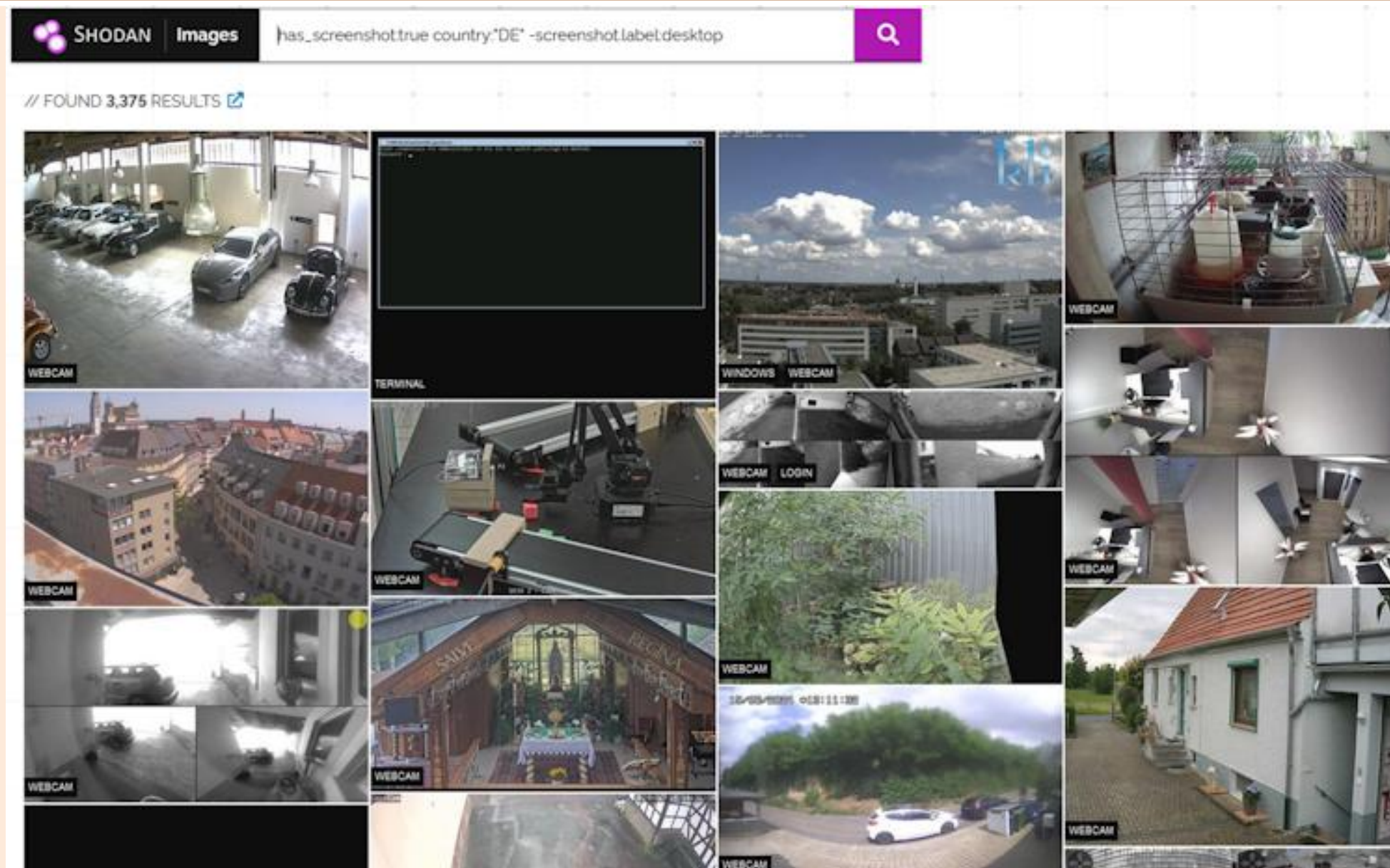
Portugal - Shodan.io - Search Engine for Internet Of Things

Webcam

THANK YOU

Q & A