Sea and Vulnerabilities as Seen by Shodan

CELFOCUS HACKATHON – 17/06/2024

PORTUGAL EDITION

$whoami

- Pedro Vieira
- Cyber Security Engineer
- Certified Ethical Hacker
- Degree at University of Minho

Disclaimer & Laws

Disclaimer
Boring but necessary

▶ Information in this presentation is intended for **educational and awareness purposes only**.

▶ **Live presentation**. Not a controlled environment and some contents may be inappropriate for some users.

▶ **I accept no responsibility** in any kind for the use, misuse, downloading, viewing in whatever way the links in this presentation.

▶ This presentation **is not related** to my work or employer.

Disclaimer
Avoid illegal activities

▶ Some links, websites, software or other items listed may or **may not be legal**, illegal, a felony, misdemeanor, or worse, in your country.

▶ Please make sure that you are **allowed** to browse the websites, download links and software **BEFORE USING!**

▶ Ignorance about laws or rules is **no excuse** for illegal activities or wrongdoing.

▶ Illegal activities may get you in **trouble or arrested**.

▶ **Always check what is legal, and what laws apply.**

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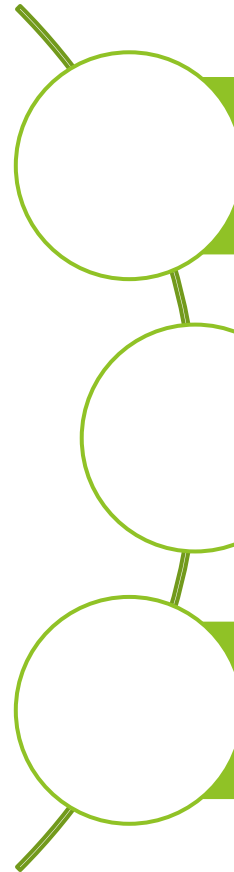
- Laws
  - Diário República Eletrónico ([link](#))
  - ANACOM ([link](#))
- Organizations
  - CNCS – Centro Nacional de Cibersegurança ([link](#))
    - Incident Notification ([link](#))
    - CERT.PT ([link](#))
  - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) ([link](#))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

Agenda

Vulnerability
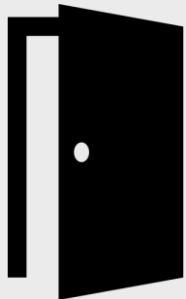
Common Attack Vectors

Portuguese Landscape

Vulnerability

Definition and Statistics

Vulnerability
Vulnerability vs incident

Vulnerability
"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

Vulnerability Statistics by Year

Vulnerabilities in NVD per Year

Year	# Vulnerabilities
2000	1 242
2001	1 556
2002	2 392
2003	1 553
2004	2 707
2005	4 766
2006	7 142
2007	6 580
2008	7 176
2009	5 040
2010	5 217
2011	4 860
2012	5 891
2013	6 780
2014	8 979
2015	8 745
2016	10 547
2017	16 979
2018	17 348
2019	16 976
2020	20 453
2021	22 304
2022	24 596
2023	26 819
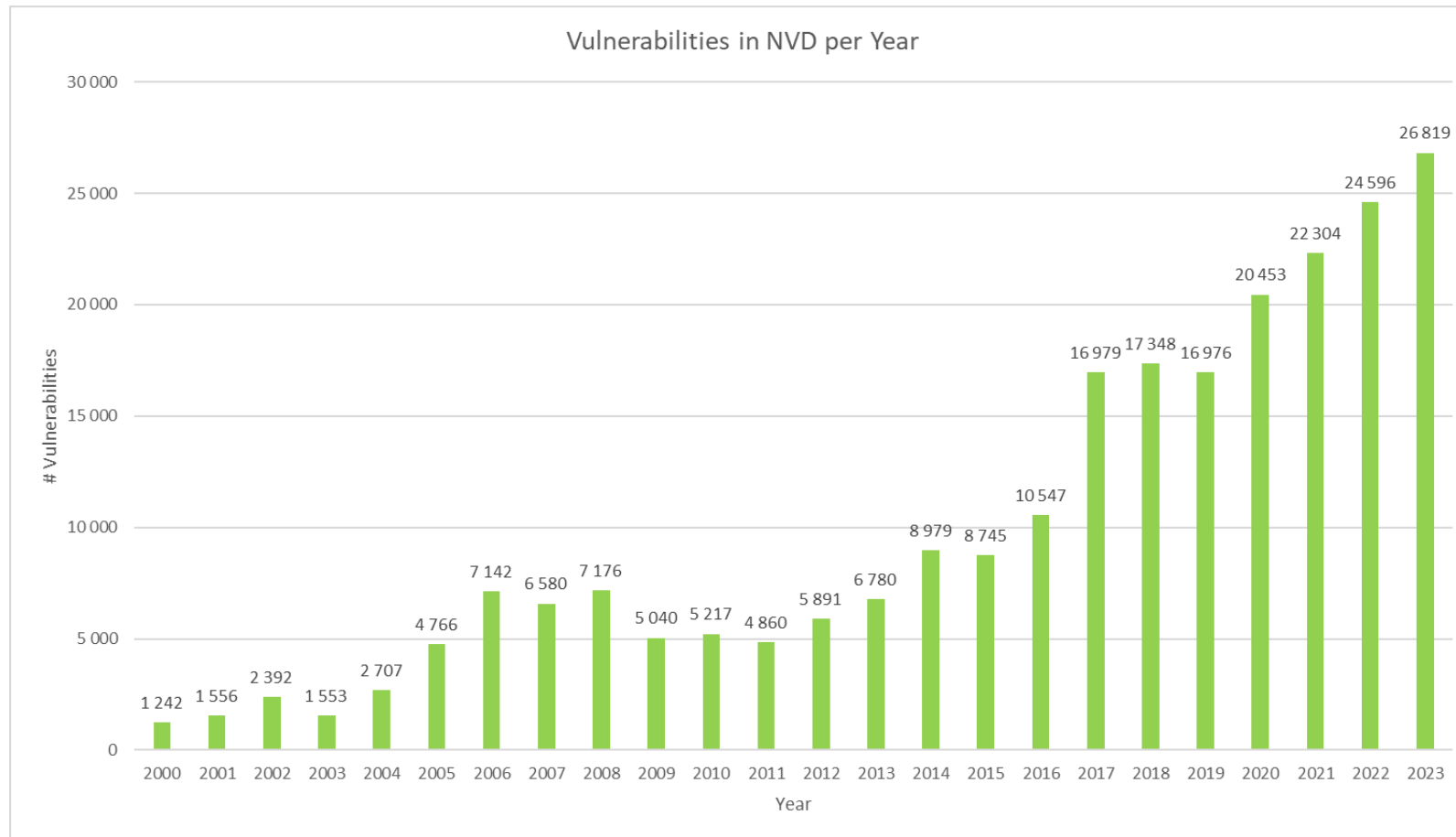
Total known vulnerabilities

283.154

Source NVD 14/03/2024

10

Vulnerability Statistics by Severity

Vulnerabilities in NVD by Severity

Severity	# Vulnerabilities
LOW	10 264
MEDIUM	112 956
HIGH	108 423
CRITICAL	32 374
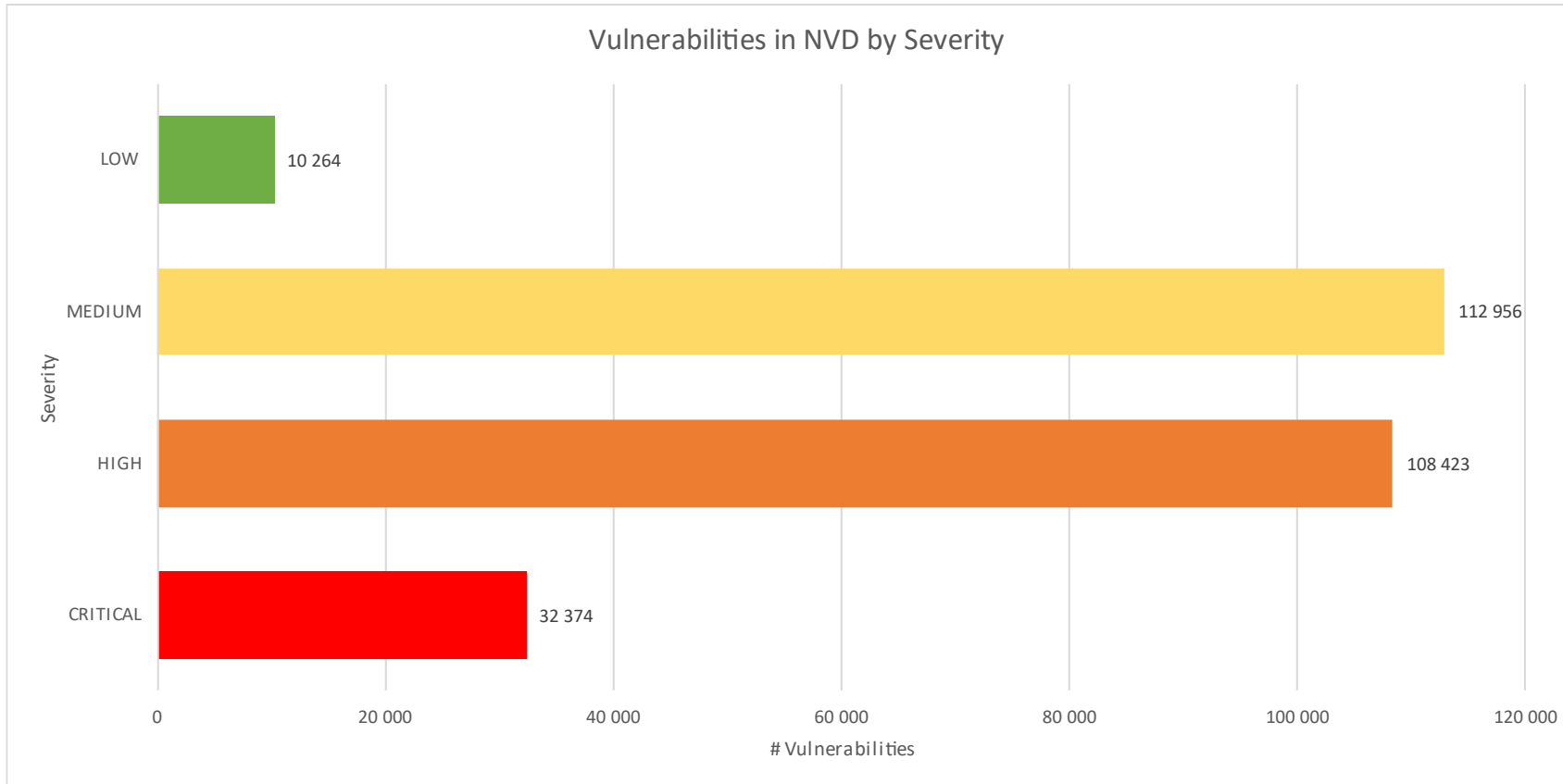
CVSS v3.1 Ratings	
LOW	0.1 - 3.9
MEDIUM	4.0 - 6.9
HIGH	7.0 - 8.9
CRITICAL	9.0 - 10.0

Source NVD 14/03/2024

11

Vulnerability
Examples from Shodan.io

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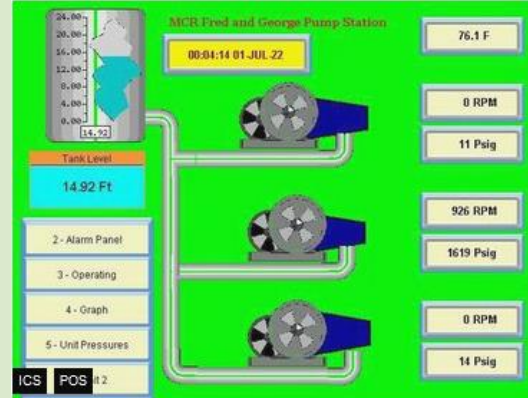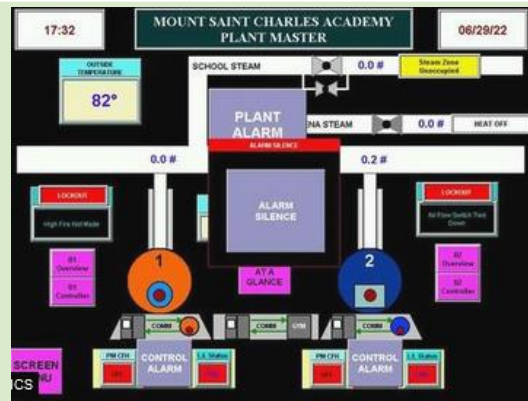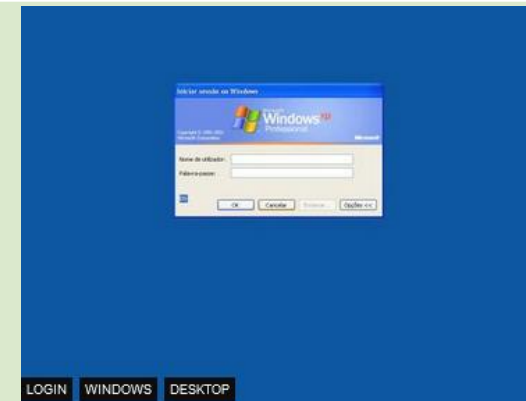
Common Attack Vectors

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

';--have i been pwned?

Check if your email address is in a data breach

email address   pwned?

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

Common Attack Vectors
Malware - Ransomware

Portuguese landscape

Portugal
Shodan.io - Search Engine for Internet Of Things
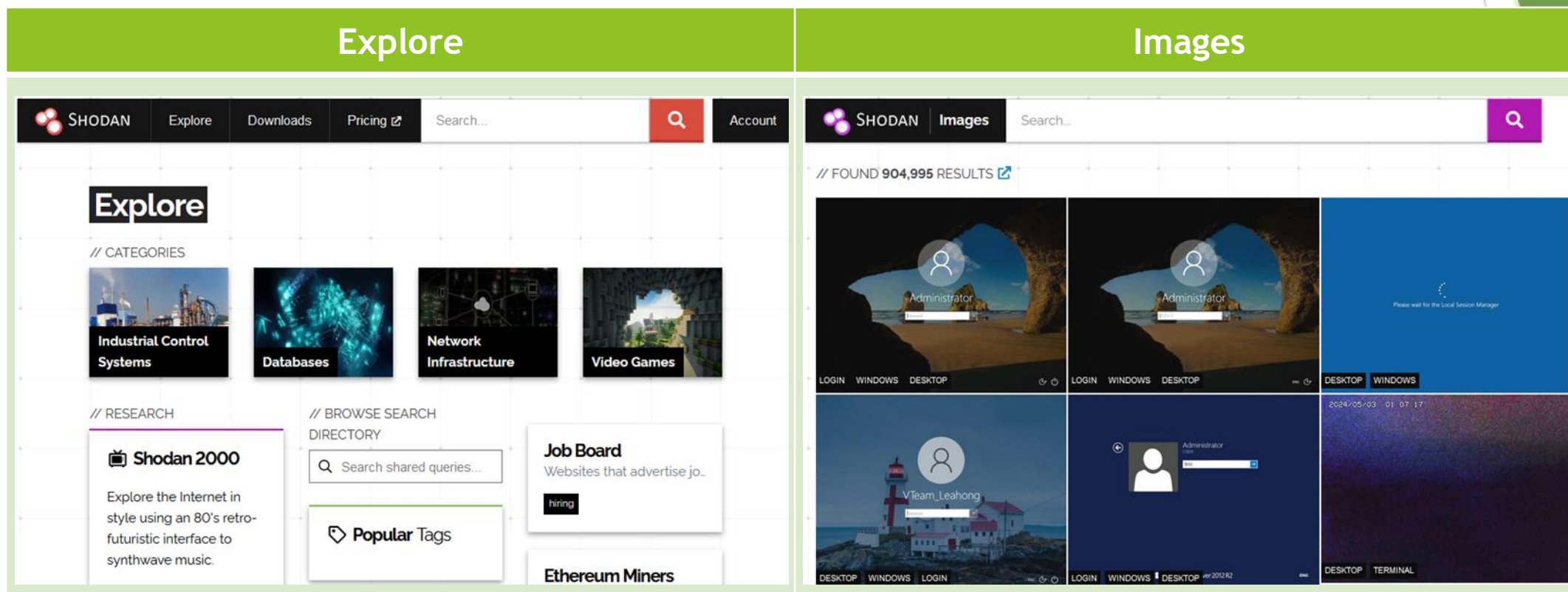
Shodan Queries ([link](#))

Portugal
Shodan.io - Search Engine for Internet Of Things

Internet Exposure Observatory

21
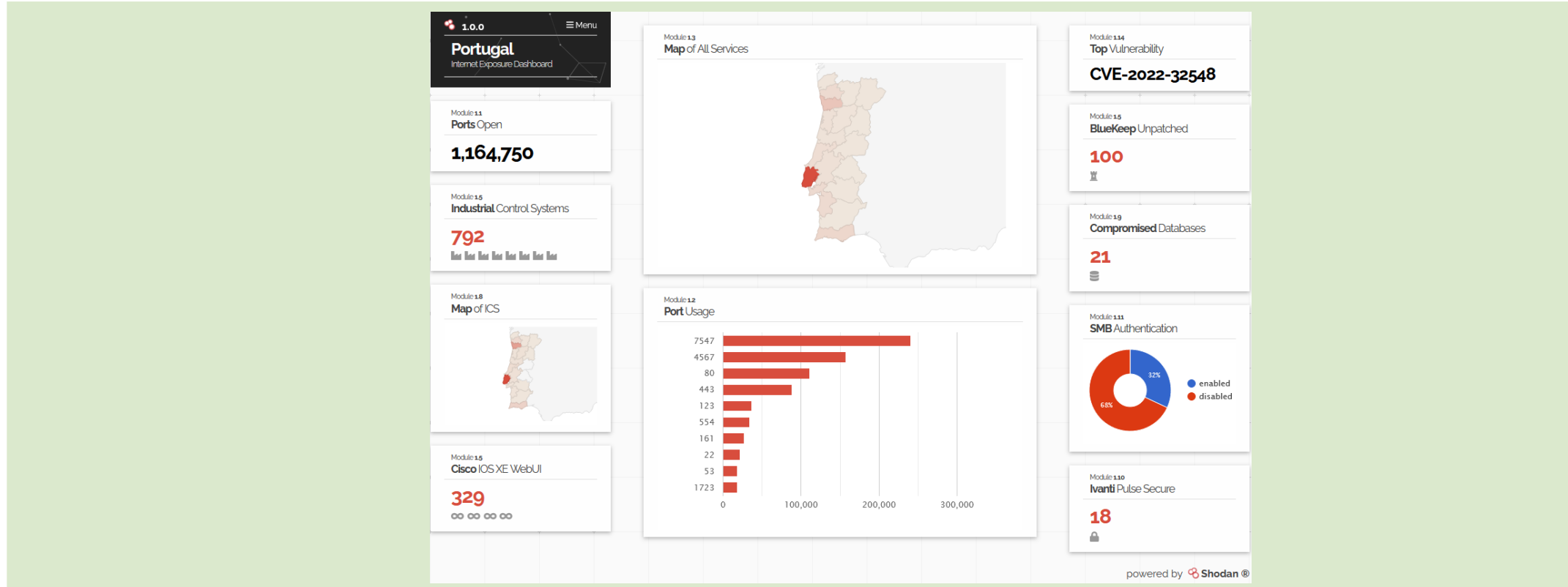
Portugal
Shodan.io - Search Engine for Internet Of Things

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

Portugal
Shodan.io - Search Engine for Internet Of Things

Portugal
Shodan.io - Search Engine for Internet Of Things

THANK YOU

Q&A