

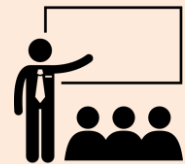
C-DAYS

2025

Agenda



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.



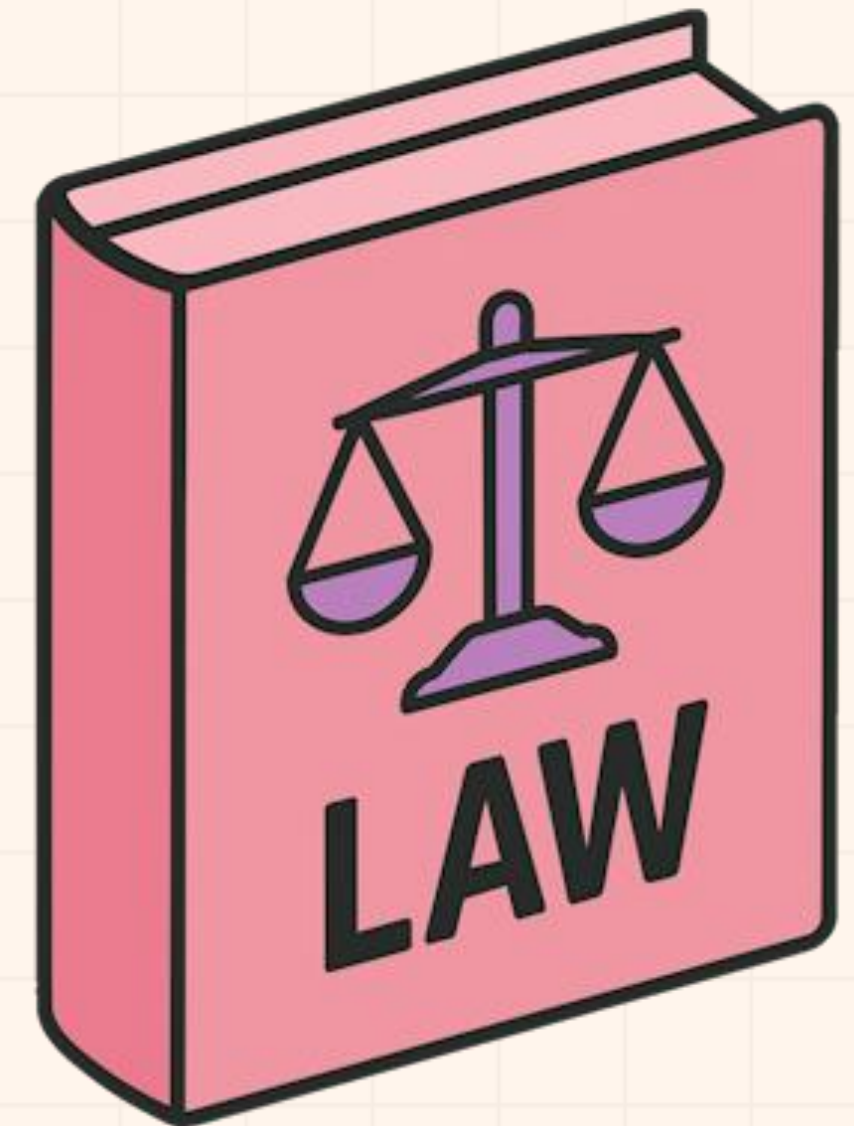
This presentation is not related to my work or employer.

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

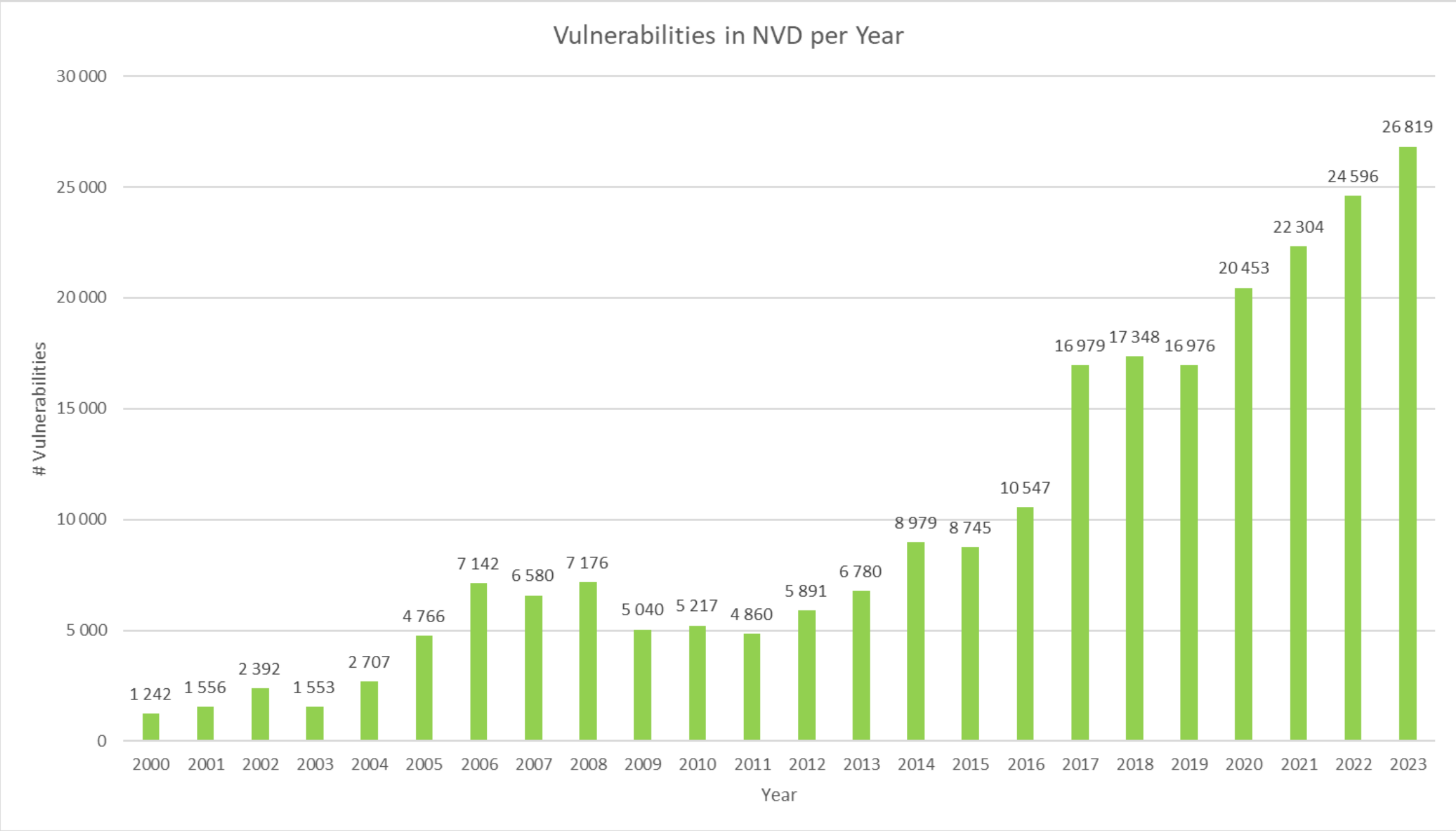
Logged In Remote Access

"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
<p>Open door</p> 	<p>Unauthorized access</p> 

Vulnerability - Statistics by Year

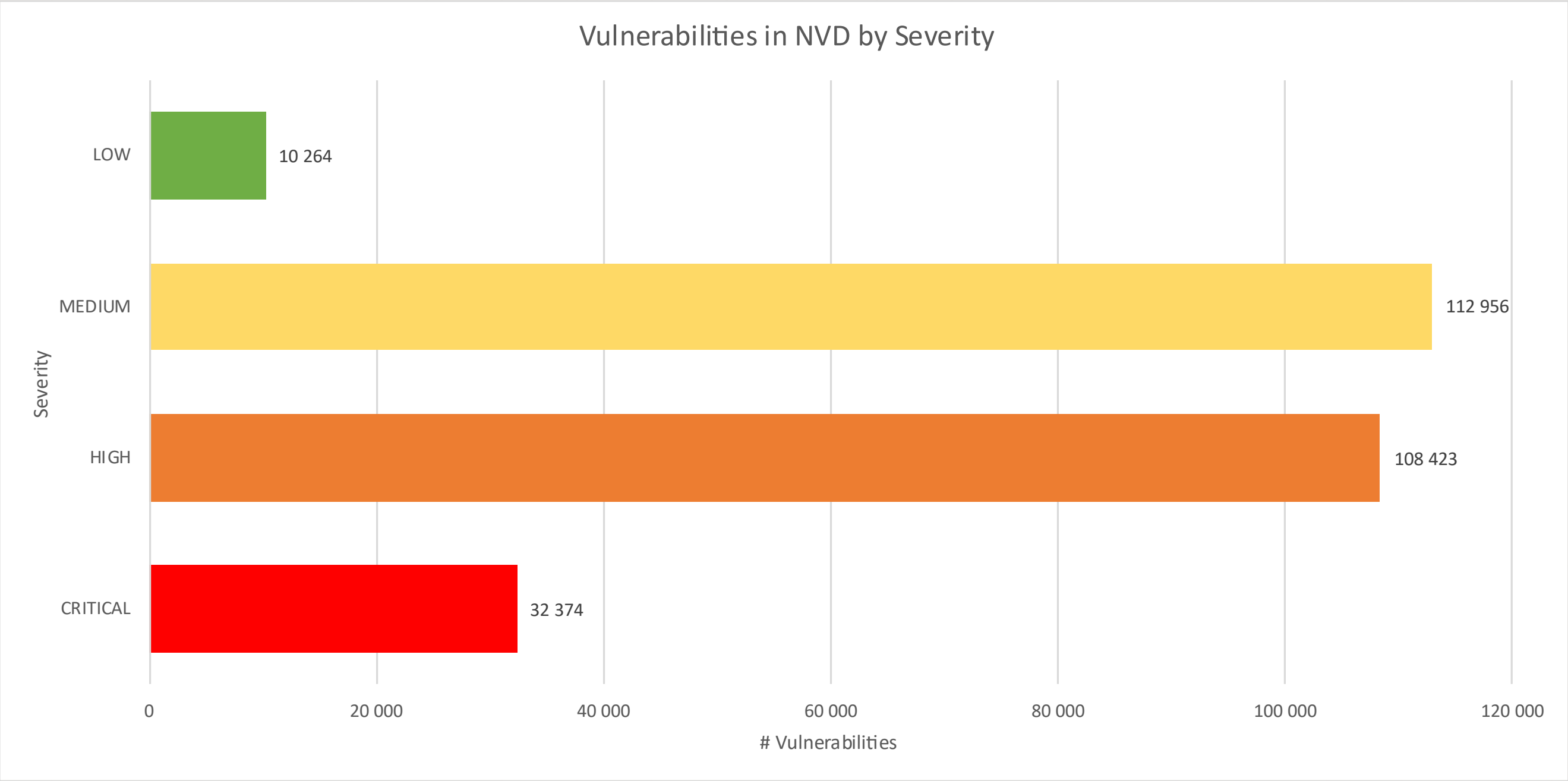


Total known vulnerabilities

283.154

Source NVD 14/03/2024

Vulnerability - Statistics 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

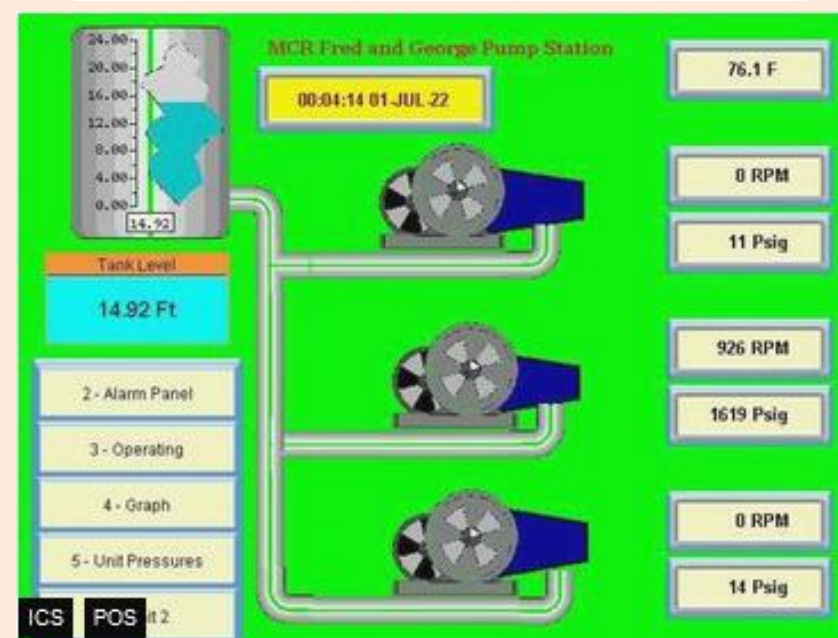
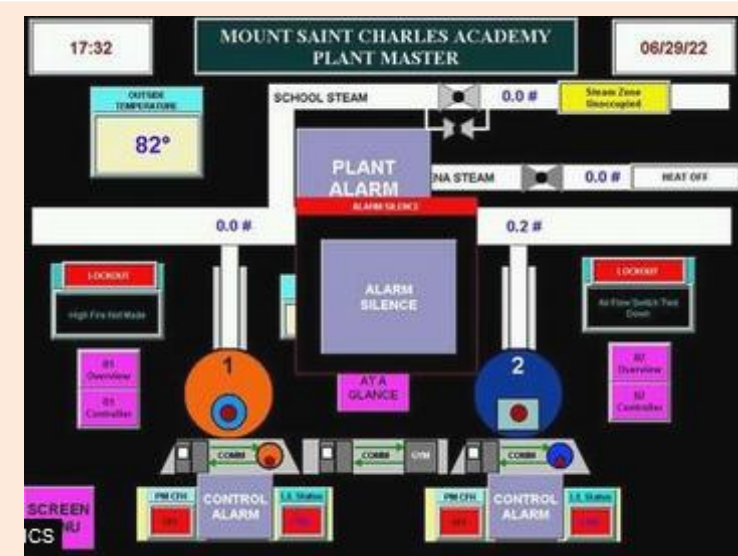
Source NVD 14/03/2024

Vulnerability - Examples from Shodan.io

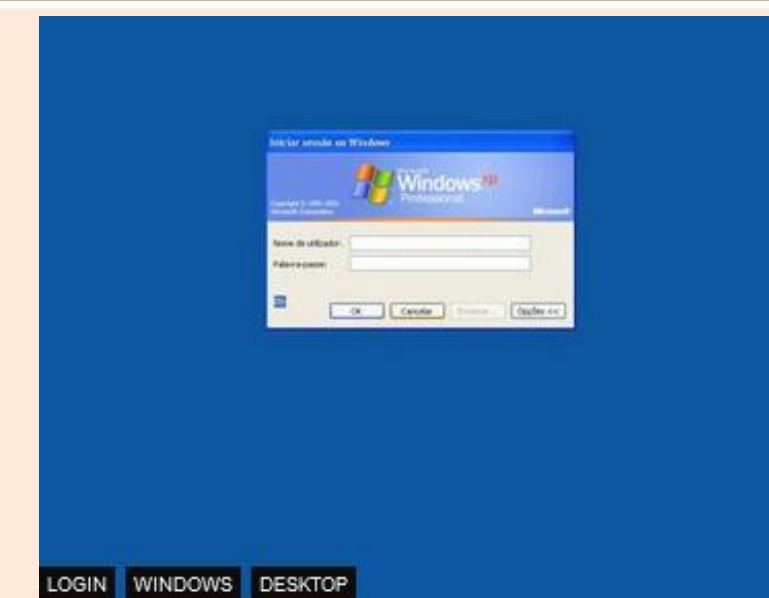
Default/No Password



Industrial Control Systems



Vulnerable Systems



Common Attack Vectors

Easy-Peasy

Common Attack Vectors - Credentials

[illegible]

Common Attack Vectors - Misconfiguration

Shared Folder – Authentication disabled

SMB Status:
Authentication: disabled
SMB Version: 2
Capabilities: raw-mode

Shares Name	Type
projetos	Disk
arquivo	Disk
administrativo	Disk
software	Disk
contabilidade	Disk
pec-cladmara	Disk
pec-helio	Disk
pec-augusto	Disk
pec-sergio	Disk
pec-antunes	Disk
pec-fabiane	Disk
pec-eng1	Disk
pec-eng2	Disk
pec-eng3	Disk
pec-eng4	Disk
print\$	Disk
IPC\$	IPC

SMB Status:
Authentication: disabled
SMB Version: 2
Capabilities: raw-mode

Shares Name	Type
Programas	Disk
FINANCEIRO	Disk
ADMINISTRATIVO	Disk
COMERCIAL	Disk
CONTABILIDADE	Disk
FATURAMENTO	Disk
FERNANDO	Disk
LABORATORIO	Disk
LOGISTICA	Disk
MARCOS	Disk
RH	Disk
Public	Disk
print\$	Disk
IPC\$	IPC

SMB Status:
Authentication: disabled
SMB Version: 2
Capabilities: raw-mode

Shares Name	Type
Multimedia	Disk
Download	Disk
Web	Disk
Public	Disk
homes	Disk
Projetos	Disk
GuardDB	Disk
GuardRecording	Disk
GuardAutoSnap	Disk
Contabilidade	Disk
Admin	Disk
Container	Disk
Browser Station	Disk
QmailAgent	Disk
Madalena	Disk
Sara	Disk
Ines	Disk
HTProjetos	Disk
PAG	Disk
home	Disk
IPC\$	IPC

WordPress site – Configuration available

WordPress › Setup Configuration File

Welcome to WordPress. Before getting started, we need some information on the database. You will need to know the following items before proceeding.

1. Database name

2. Database username

3. Database password

4. Database host

5. Table prefix (if you want to run more than one WordPress in a single database)

We're going to use this information to create a wp-config.php file. **If for any reason this automatic file creation doesn't work, don't worry. All this does is fill in the database information to a configuration file. You may also simply open wp-config-sample.php in a text editor, fill in your information, and save it as wp-config.php.** Need more help? [We got it.](#)

In all likelihood, these items were supplied to you by your Web Host. If you don't have this information, then you will need to contact them before you can continue. If you're all ready...

Let's go!

Common Attack Vectors - Software Vulnerabilities

Shared Folder - Remote Code Execution

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.

SMB Status:

Authentication: disabled

SMB Version: 2

Capabilities: raw-mode

Shares		
Name	Type	Comments
ADMIN\$	Disk	Admin remoto
C\$	Disk	Partilha predefinida
credTec	Disk	
D\$	Disk	Partilha predefinida
Executavel	Disk	
IPC\$	IPC	IPC remoto
passagem	Disk	
PHCSistema	Disk	
Users	Disk	
validacc	Disk	

Website – Several vulnerabilities

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA

TODOS CONTAM


PLANEAR O ORÇAMENTO FAMILIARFAZER PAGAMENTOSPOUPAR E INVESTIRCRIAR UMA EMPRESA

CONCURSO
O MEU F
FINANCE

ETAPAS DA VIDA

ESTUDARCOMEÇAR A TRABALHARCOMPRAR CARROCOMPRAR CASACONSTITUIR FAMÍLIA

ORÇAMENTOSIMULADORCRÉDITO ÀCRÉDITO A

 Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-45802

5.9

When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVE-2023-31122

7.5

Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

CVE-2023-25690

9.8

Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?\$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

CVE-2022-37436

5.3

Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

CVE-2022-36760

9.0

Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

Common Attack Vectors - Malware - Ransomware

Redeemer Ransomware	Ransomwatch
<div><div>Redeemer Ransomware - Your Data Is Encrypted</div><div>8888888b. 888 888 Y88b 888 888 888 888 888 d88P .d88b. .d88888 .d88b. .d88b. 88888b.d88b. .d88b. 888d888 88888888P" d8P Y8b d88" 888 d8P Y8b d8P Y8b 888 "888 "88b d8P Y8b 888P" 888 T88b 88888888 888 888 88888888 88888888 888 888 888 88888888 888 888 T88b Y8b. Y88b 888 Y8b. Y8b. 888 888 888 Y8b. 888 888 T88b "Y8888 "Y88888 "Y8888 "Y8888 888 888 888 "Y8888 888</div><div>Made by Cerebrate Visit the official Redeemer Ransomware Tor website - redeemergd6gjtzgjuif5jgpkk6i3xybkhsldzjoyjaxivyZlnhvmzcad.onion</div><div><div>[Question 1] What happened to my computer? I cannot access my files and they have changed their extension?</div><div>[Answer 1] Your files have been encrypted by Redeemer, a Darknet ransomware operation.</div></div><div><div>[Question 2] Is there any way to recover my files?</div><div>[Answer 2] Yes, you can recover your files. This will however cost you money in Monero (XMR).</div></div><div><div>[Question 3] Is there any way to recover my files without paying?</div><div>[Answer 3] Without paying for the proper decryption key, you will NEVER regain access to your files. Redeemer uses the most secure algorithms and a sophisticated encryption scheme which guarantees security. Ever since Redeemer was first released publicly (~May 2021) no one managed to crack the decryption or recover their files without paying.</div></div><div>OK</div></div>	<div><div>summary</div><div>may 4th, 2024</div><div>ransomwatch is currently crawling 382 sites belonging to 192 unique groups</div><div><div>🕒</div>there have been 31 posts within the last 24 hours</div><div><div>🗓️</div>there have been 64 posts within the month of may</div><div><div>📅</div>there have been 1286 posts within the last 90 days</div><div><div>🗓️</div>there have been 1712 posts within the year of 2024</div><div><div>⚙️</div>there are currently 100 online hosts & 120 custom parsers.</div><div><div>🕒</div>ransomwatch has been running for 2 years, 7 months and 28 days and indexed 11169 posts</div><div>all data (<u>groups</u>) and (<u>posts</u>) is available in JSON (updated hourly)</div><div>ransomwatch is fully <u>open source</u>. please consider <u>sponsoring</u> if you find it useful!</div></div>

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

Ransomwatch

recent posts

last 200 posts

date	title	group
2024-05-04	firstmac.com.au	embargo
2024-05-04	mulfordconstruction.com	embargo
2024-05-04	bulldogbag.com	underground
2024-05-04	frenckengroup.com	underground
2024-05-04	synology.com	underground
2024-05-04	tpa-group.sk	underground
2024-05-04	Triathlon.group	underground
2024-05-04	awwg.com	underground
2024-05-04	kc.co.kr	underground
2024-05-04	Y. Hata & Co., Ltd.	underground
2024-05-04	Skender Construction	underground
2024-05-04	Creative Business Interiors	underground
2024-05-04	cochraneglobal.com	underground
2024-05-04	ikfhomefinance.com	darkvault
2024-05-04	The Islamic Emirat of Afghanistan National Environmental Protection Agency <nepa.gov.af/df	ransomhub
2024-05-04	Accounting Professionals LLC. Price, Breazeale &#038; Chastang	everest
2024-05-04	Bitfinex	flocker
2024-05-04	SBC Global	flocker
2024-05-04	Rutgers University	flocker
2024-05-04	Coinmoma	flocker

NoMoreRansom

<🔒/> NO MORE RANSOM

NEED HELP

unlocking your digital life without paying your attackers*?

YESNO

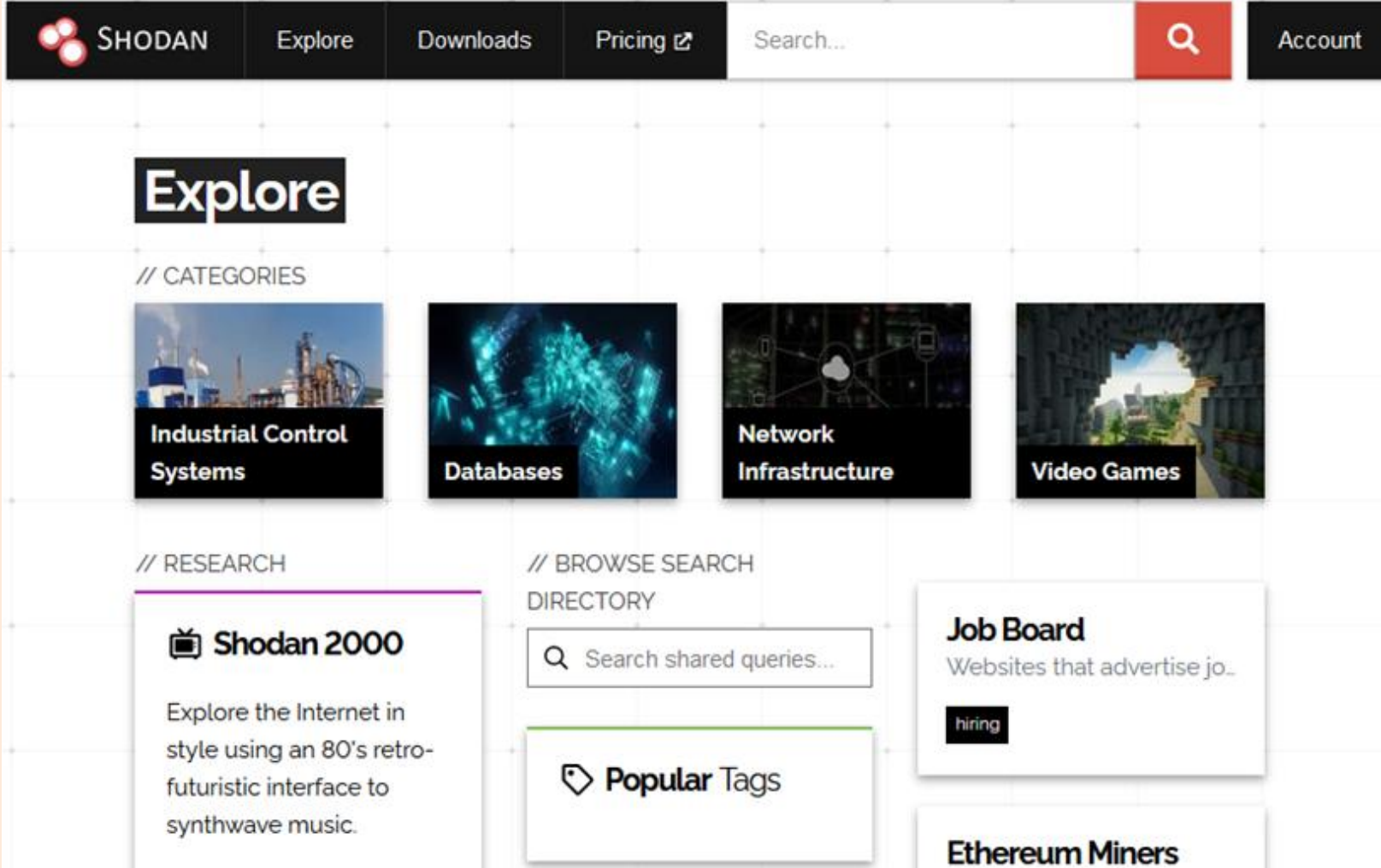
At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

Portuguese landscape

Definition and Statistics

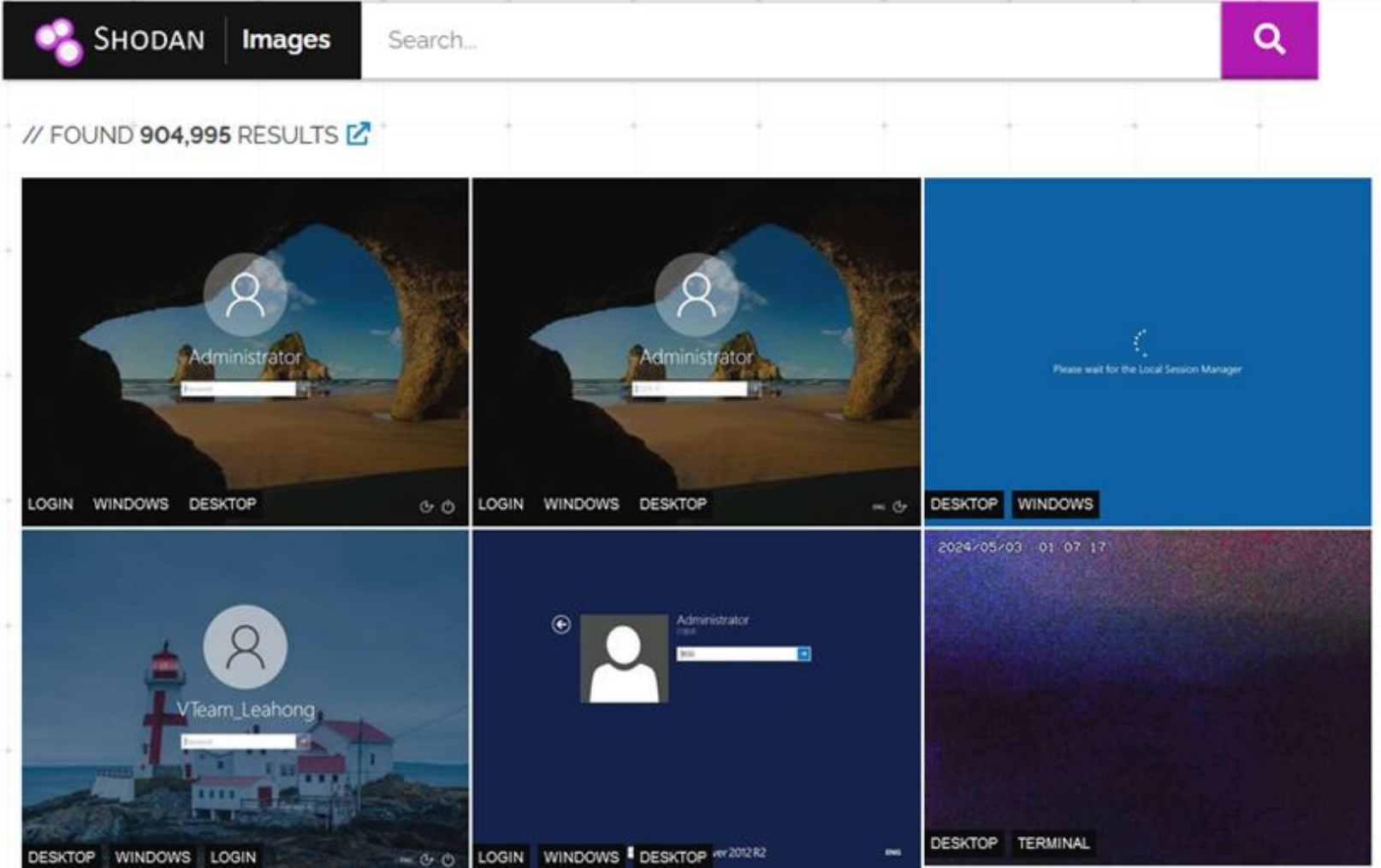
Portugal - Shodan.io - Search Engine for Internet Of Things

Explore



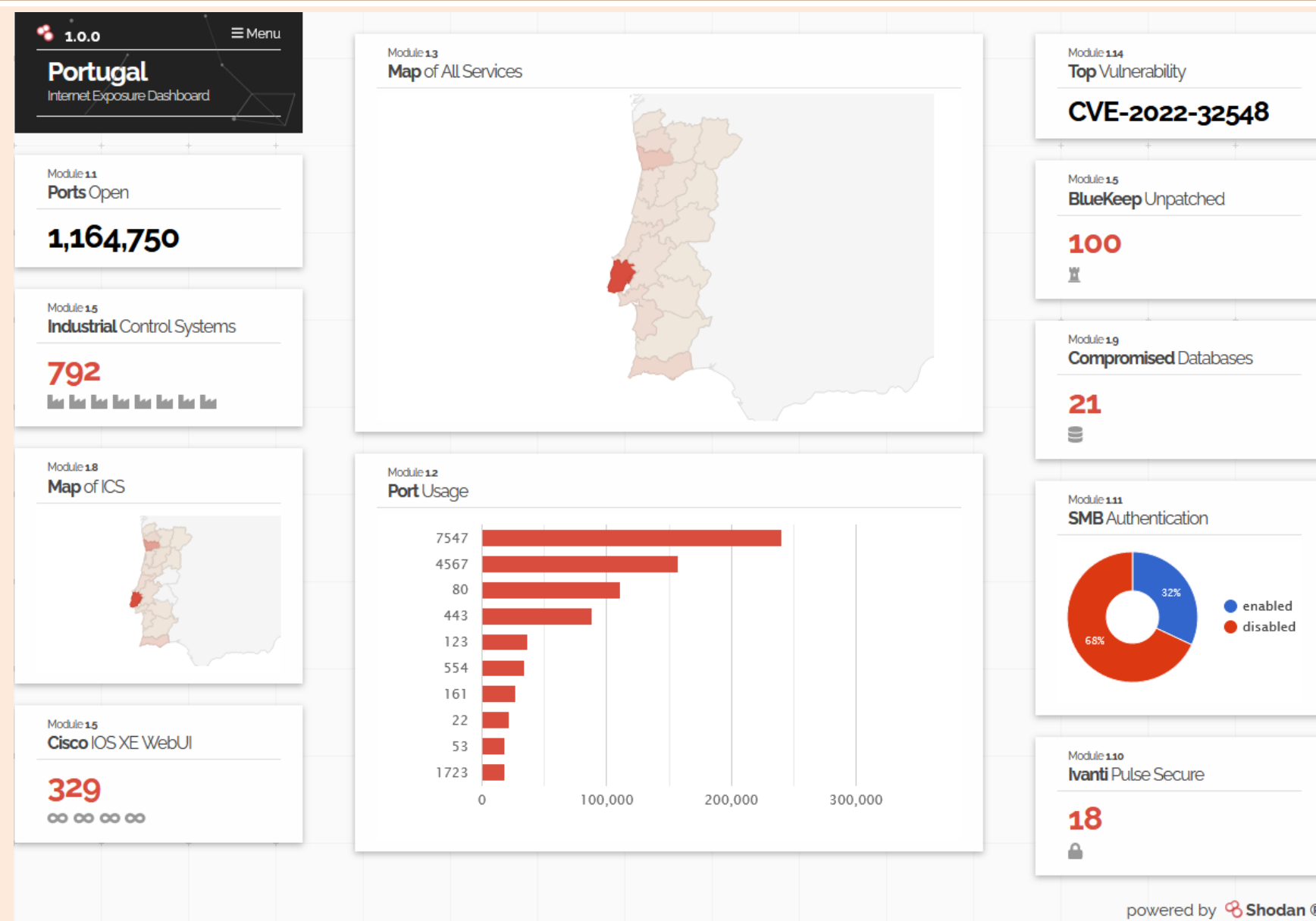
Shodan Queries ([link](#))

Images



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

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...](#)

EternalBlue - MS17-010 - CVE-2017-0144

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

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...](#)

SMBGhost - CVE-2020-0796

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

 Vulnerabilities

CVE-2019-0708

10.0

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

TOTAL RESULTS

99


TOP CITIES


Lisbon	30
Porto	11
Braga	5
Leiria	3
Espinho	2
More...	


SHODAN

Images

|vuln:CVE-2019-0708 country:pt




// FOUND 71 RESULTS 



DESKTOP

WINDOWS


LOGIN



LOGIN

WINDOWS


DESKTOP



DESKTOP

WINDOWS


LOGIN



LOGIN

WINDOWS


DESKTOP



DESKTOP

WINDOWS

LOGIN



DESKTOP

WINDOWS

LOGIN

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

Shared Folders

TOTAL RESULTS

4,261

TOP CITIES

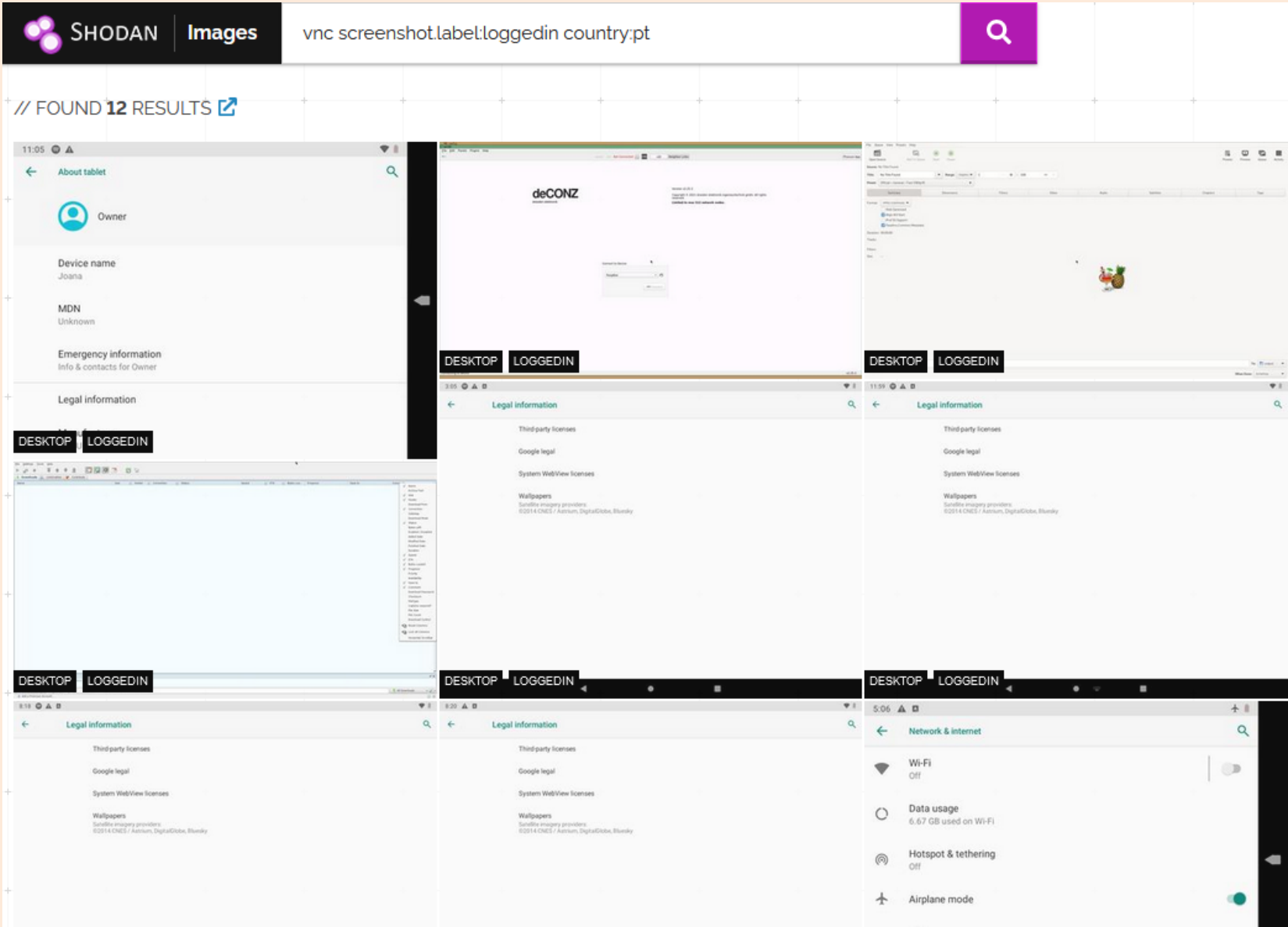
Lisbon	518
Porto	154
Braga	102
Vila Nova de Gaia	86
Coimbra	85

[More...](#)

Shares			Shares		
Name	Type	Comments	Name	Type	Comments
Web	Shares		ADMIN\$	Disk	Remote Admin
Public	Name	Type	C\$	Disk	default share
homes			IPC\$		
SCAN	Multimedia	Shares	Printer		
SERVER	Download	Name	IPC		
Multimedia	Web				
Recordings	Public	Multimedia			
home	homes	Download			
MBPT	TESTE	Web			
PLOUTOS	JOAO	Public			
TGS	DUDA	homes			
MIRUS	SEGMENTO_POPULAR	BackupR			
USB	SOFTWARE	home			
IPC\$	home	IPC\$			
	IPC\$				

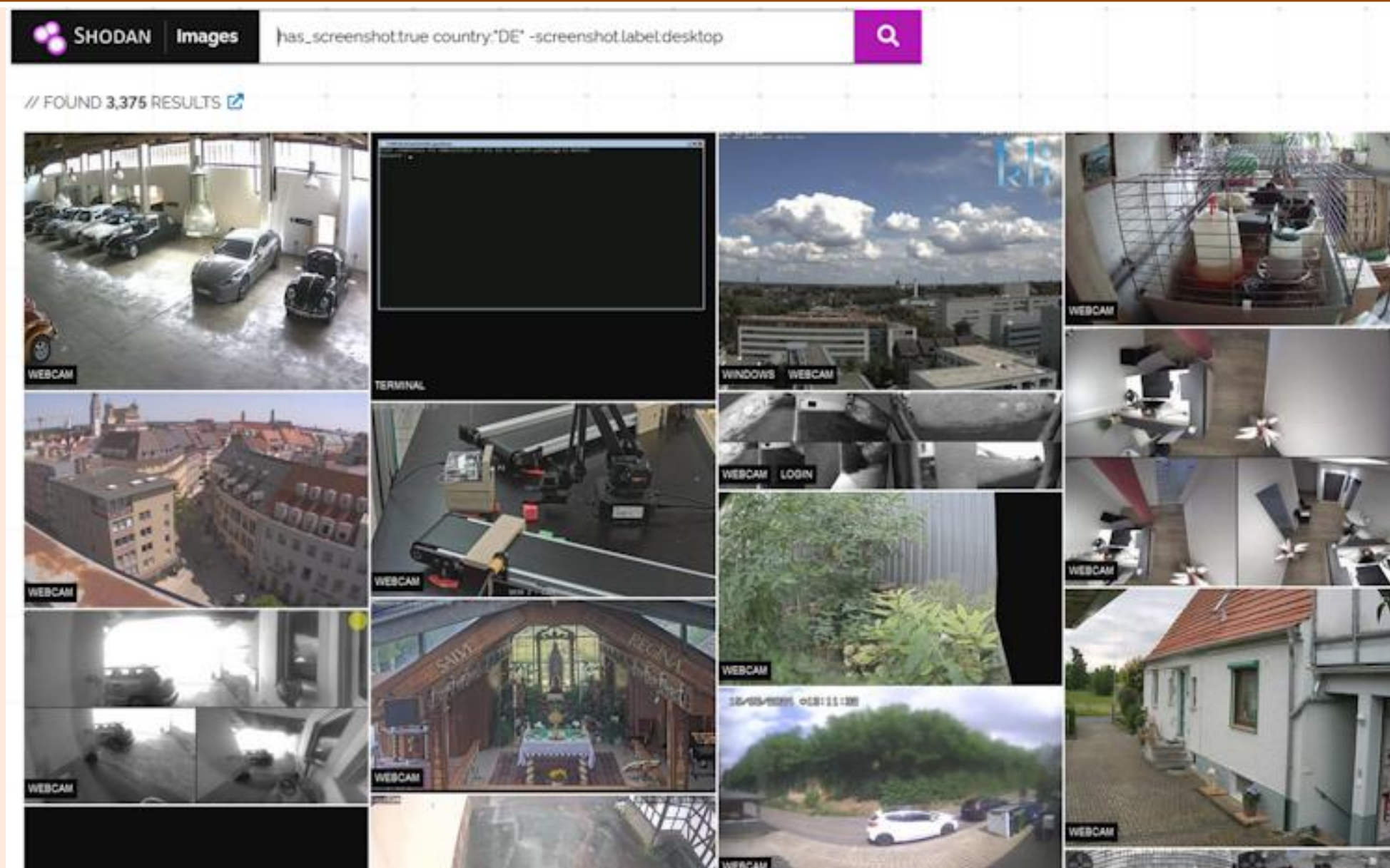
Portugal - Shodan.io - Search Engine for Internet Of Things

TOTAL RESULTS	
12	
TOP CITIES	
Porto	8
Lisbon	2
Cacém	1
Vila Nova de Gaia	1



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

Webcam



THANK YOU

Q & A

