Deutschland
Bier, Wurst und Schwachstellen

Open Identity Summit 2024

$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**.

▶ <u>**Always check what is legal, and what laws apply.**</u>
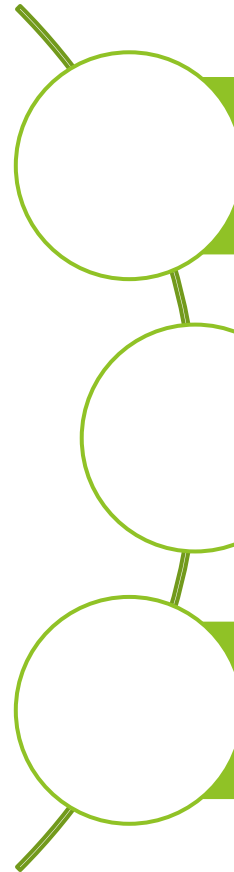
Laws
Portuguese Law and Organizations

- 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

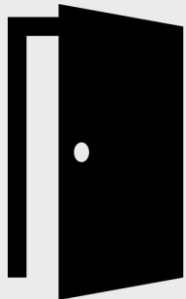Portuguese Landscape

Vulnerability

Definition and Statistics
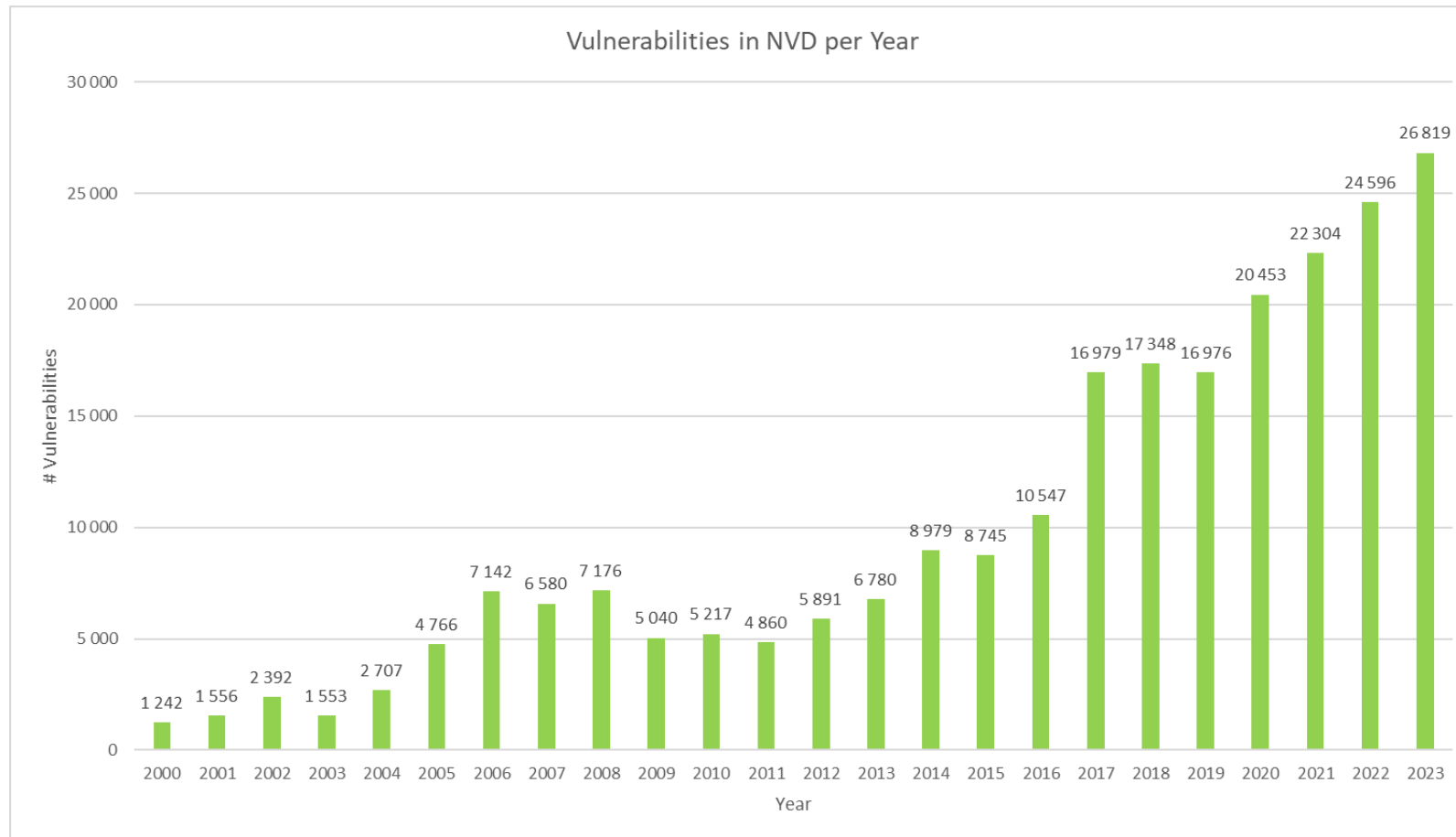
Vulnerability
Vulnerability vs incident

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

Total known vulnerabilities

283.154

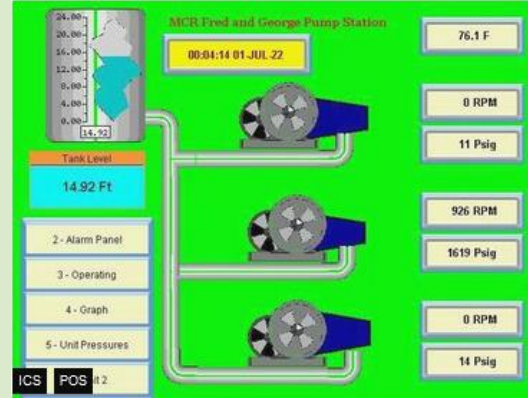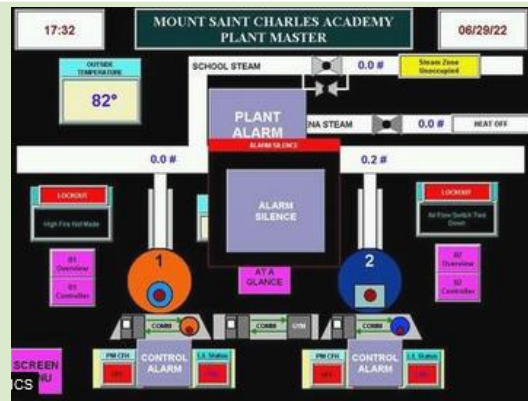# Vulnerability Statistics by Severity
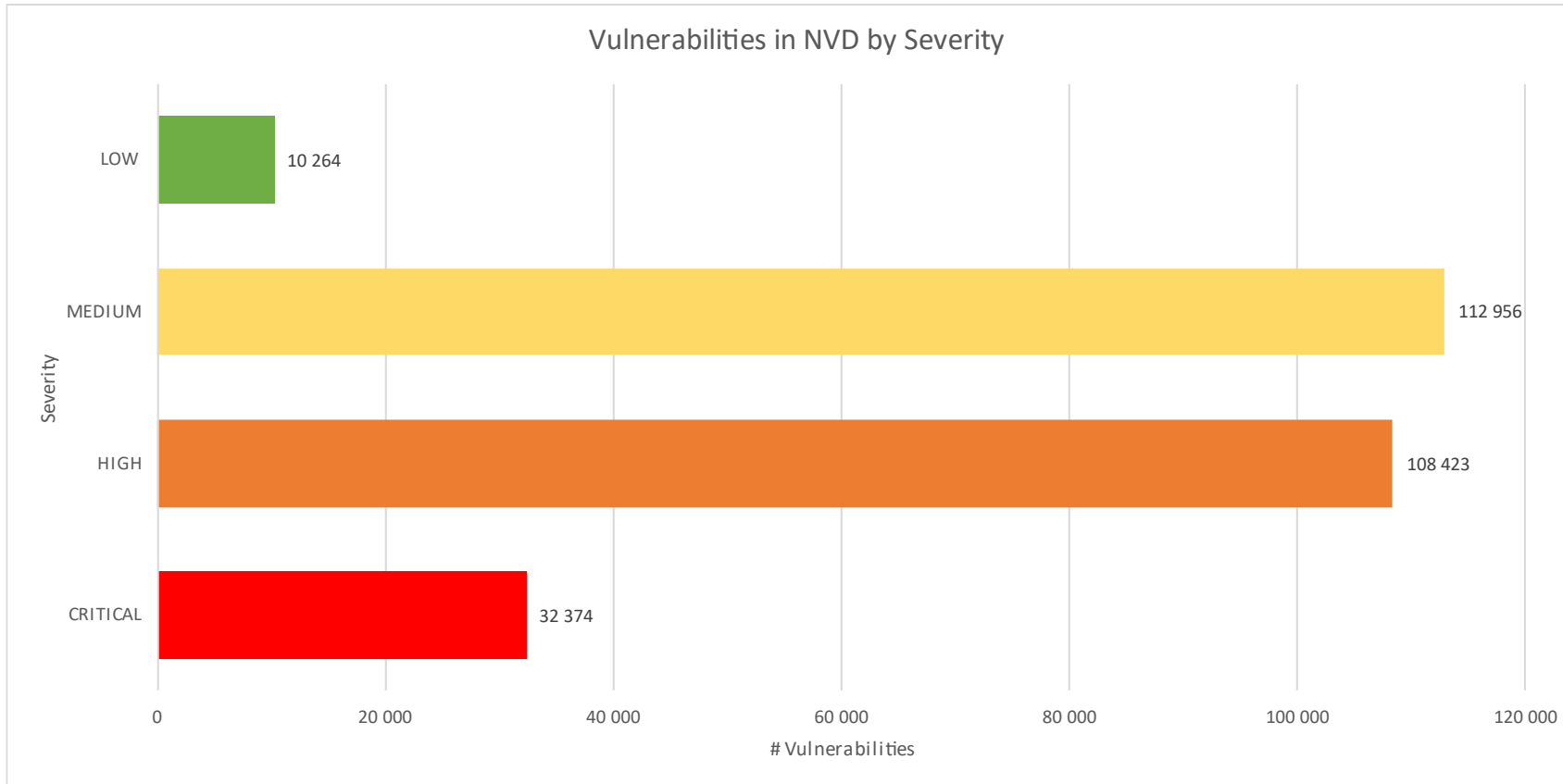
Vulnerability
   Examples from Shodan.io

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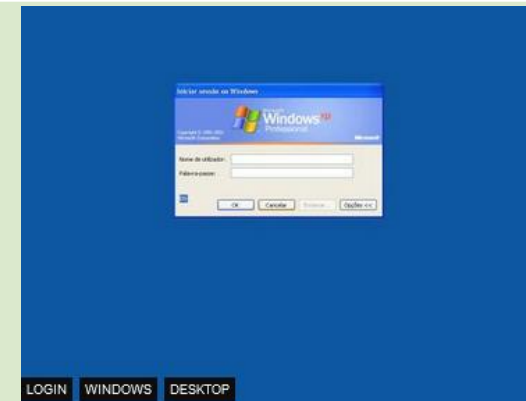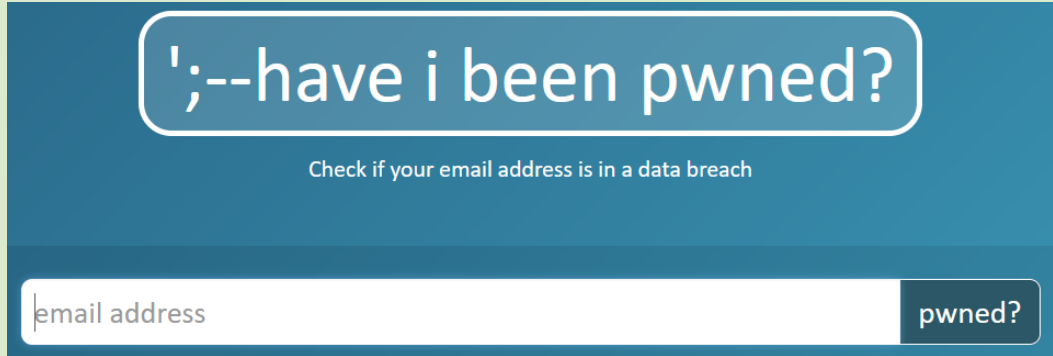
Common Attack Vectors

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

⚠ **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
```

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA

TODOS CONTAM

PLANEAR O ORÇAMENTO FAMILIAR | FAZER PAGAMENTOS | POUPAR E INVESTIR

CONCURSO
O ME
FINAN

ETAPAS DA VIDA
- ESTUDAR
- COMEÇAR A TRABALHAR
- COMPRAR CARRO
- COMPRAR CASA
- CONSTITUIR FAMÍLIA

⚠ **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 ServerThis 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 `6.3` 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
Redeemer Ransomware - Your Data Is Encrypted Made by Cerebrate Visit the official Redeemer Ransomware Tor website - redeemergd6gjtzgiuf5jgpkk6i3xybkhsldzjoyjaxivyzlnhvmzcad.onion [Question 1] What happened to my computer? I cannot access my files and they have changed their extension? [Answer 1] Your files have been encrypted by Redeemer, a Darknet ransomware operation. [Question 2] Is there any way to recover my files? [Answer 2] Yes, you can recover your files. This will however cost you money in Monero (XMR). [Question 3] Is there any way to recover my files without paying? [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. OK	summary may 4th, 2024 ransomwatch is currently crawling 382 sites belonging to 192 unique groups ⊙ there have been 31 posts within the last 24 hours there have been 64 posts within the month of may there have been 1286 posts within the last 90 days there have been 1712 posts within the year of 2024 there are currently 100 online hosts & 120 custom parsers. ransomwatch has been running for 2 years, 7 months and 28 days and indexed 11169 posts all data (groups) and (posts) is available in JSON (updated hourly) ransomwatch is fully open source. please consider sponsoring if you find it useful!

Common Attack Vectors
Malware - Ransomware

Ransomwatch	NoMoreRansom

Portuguese landscape

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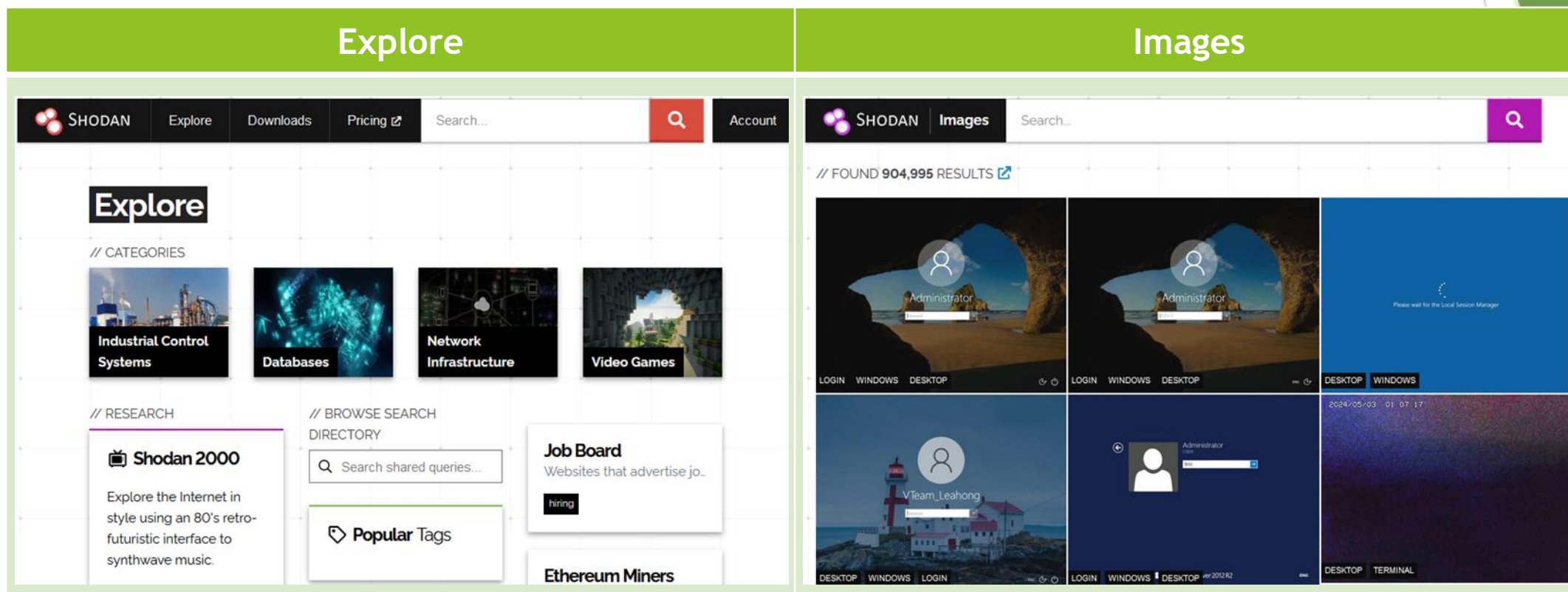
Shodan Queries (link)

Portugal
Shodan.io - Search Engine for Internet Of Things

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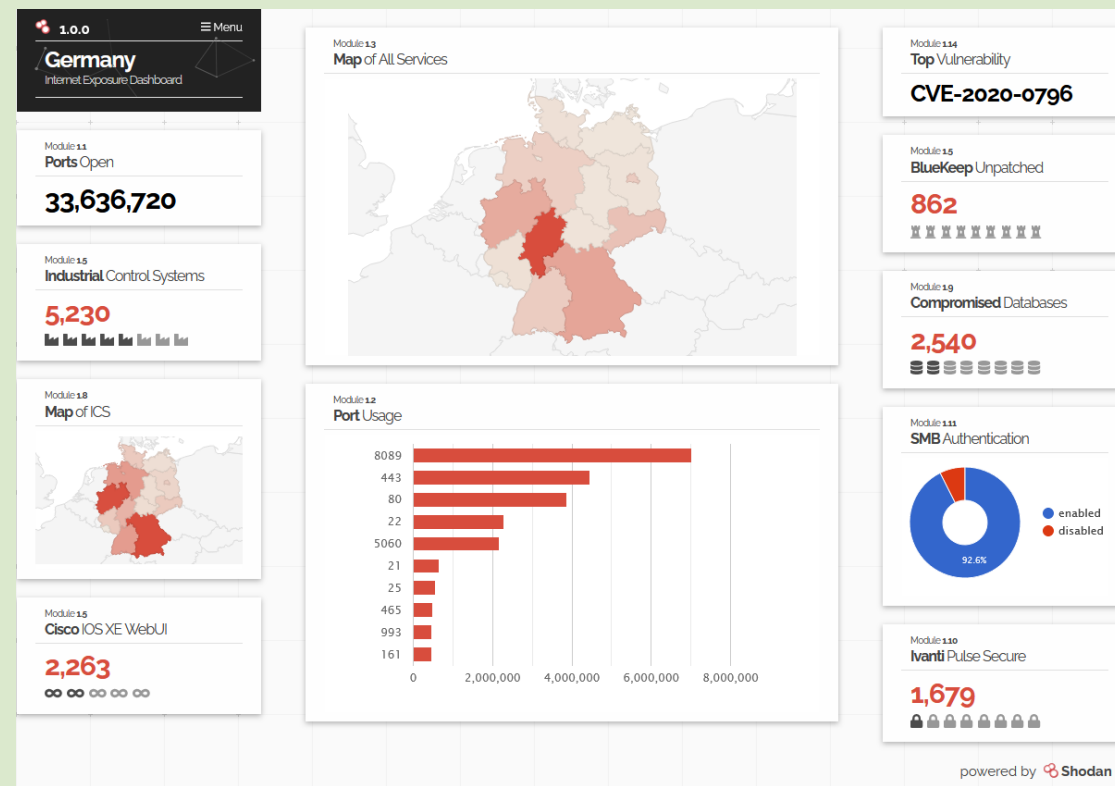
Portugal
Shodan.io - Search Engine for Internet Of Things

Top in Germany - SMBGhost - CVE-2020-0796	EternalBlue - MS17-010 - CVE-2017-0144

⚠ **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.

⚠ **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

22,735

TOP CITIES

Berlin	7,836
Frankfurt am Main	5,048
Falkenstein	3,806
Düsseldorf	3,075
Nürnberg	1,340
More...	

TOTAL RESULTS

215

TOP CITIES

Nürnberg	86
Frankfurt am Main	67
Falkenstein	26
Berlin	8
Düsseldorf	6
More...	

Portugal
Shodan.io - Search Engine for Internet Of Things

Heartbleed - CVE-2014-0160	Logjam - CVE-2022-32548

⚠ **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

4,844

TOP CITIES

Frankfurt am Main	973
Falkenstein	836
Berlin	732
Karlsruhe	413
Nürnberg	235

More...

⚠ **Vulnerabilities**

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

TOTAL RESULTS

4,225

TOP CITIES

Berlin	330
Hamburg	149
Frankfurt am Main	145
Düsseldorf	107
Munich	102

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'.
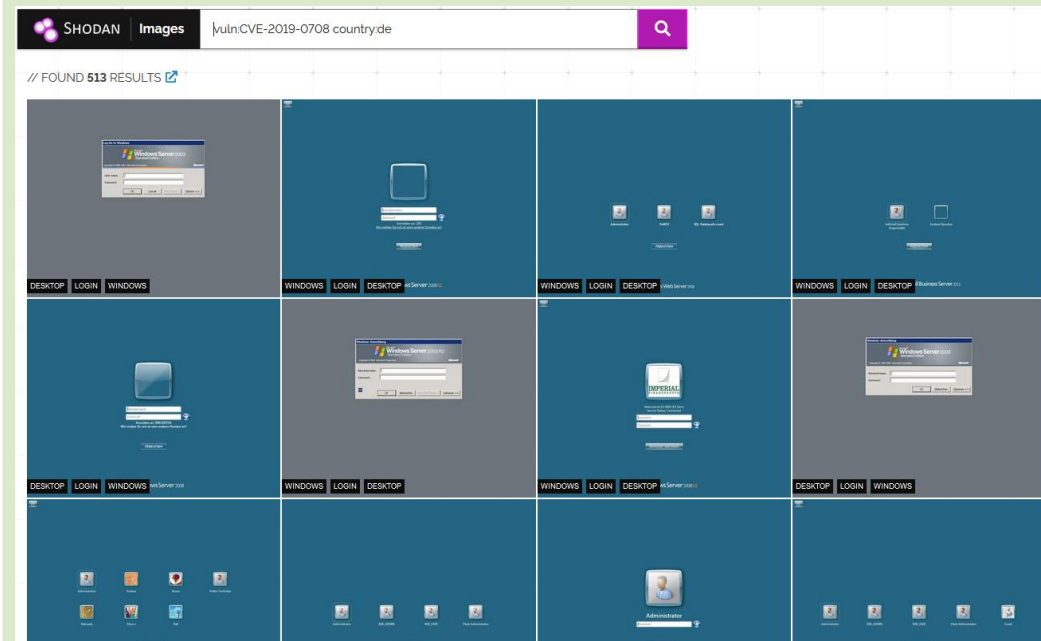
TOTAL RESULTS

905

TOP CITIES

Frankfurt am Main	234
Berlin	154
Düsseldorf	68
Falkenstein	63
Nürnberg	40

More...

SHODAN | Images | vuln:CVE-2019-0708 country:de

// FOUND **513** RESULTS

Portugal
Shodan.io - Search Engine for Internet Of Things

Shared Folders

TOTAL RESULTS

5,044

TOP CITIES

Frankfurt am Main	1,616
Falkenstein	788
Nürnberg	646
Düsseldorf	516
Berlin	469

More...

```
Shares

Name              Type          Comments
-------------------------------------------------
print$            Disk          Printer Drivers
lobby             Disk          Lobby
freebuild         Disk          Freebuild
creative          Disk          Creative
redstone          Disk          Redstone-Server
hardcore          Disk          Hardcore-Server
iron              Disk          Iron-Server
backup            Disk          Goliath
IPC$              IPC           IPC Ser
```

```
Shares

Name              Type          Comments
-------------------------------------------------
seskayit          Disk          Ses Kayitlari
faks              Disk          Faks Kayitlari
moh               Disk          Bekletme Muzikleri
sesler            Disk          Sistem Ek Mesajlari
IPC$              IPC           IPC Service (IPS File Server)
```

```
Shares

Name              Type          Comments
-------------------------------------------------
backup            Disk          Intra2net Business Server backup
restore           Disk          Intra2net Business Server backup restore
IPC$              IPC           IPC Service (Intra2net - i2n)
```
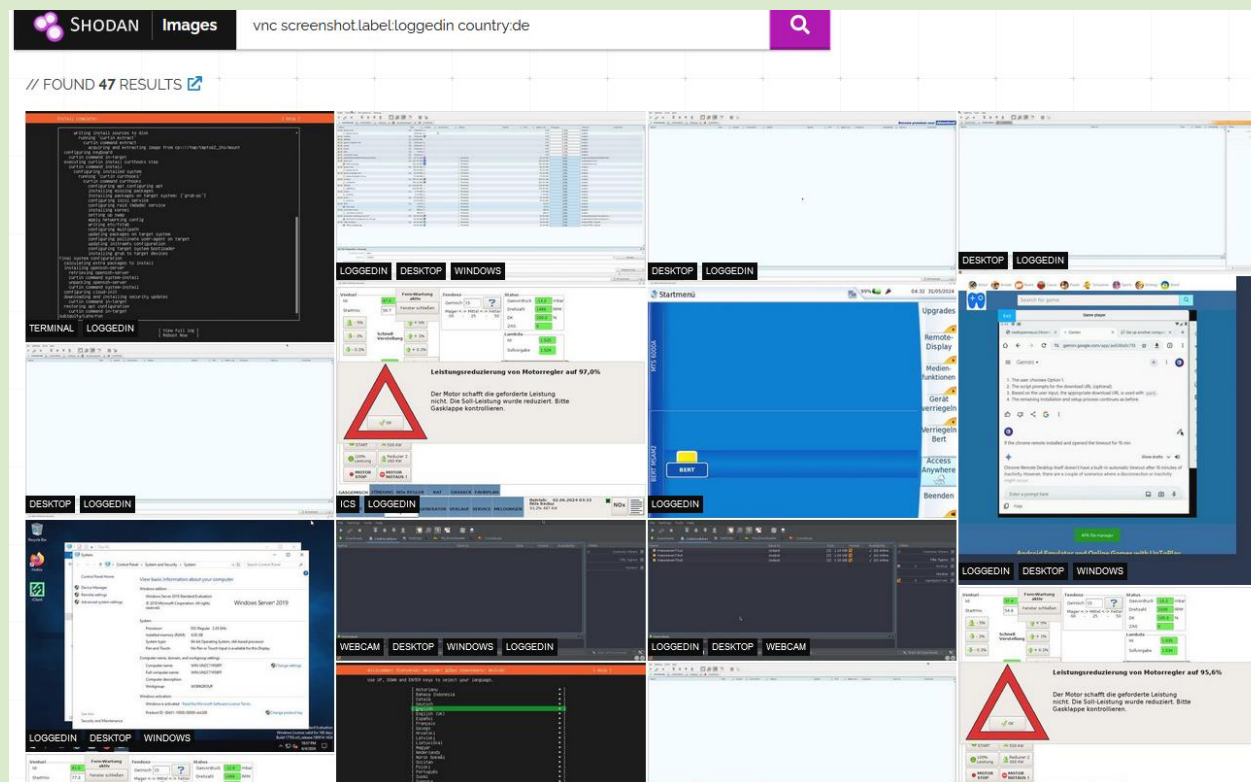
```
Shares

Name              Type          Comme
-------------------------------------------------
ADMIN$
C$
IPC$
```

```
Shares

Name              Type          Comments
-------------------------------------------------
logs              Disk          The recieved log files from customers.
IPC$              IPC           IPC Service (Ubuntu-1804-bionic-64-minimal server (Samba, Ubuntu))
```
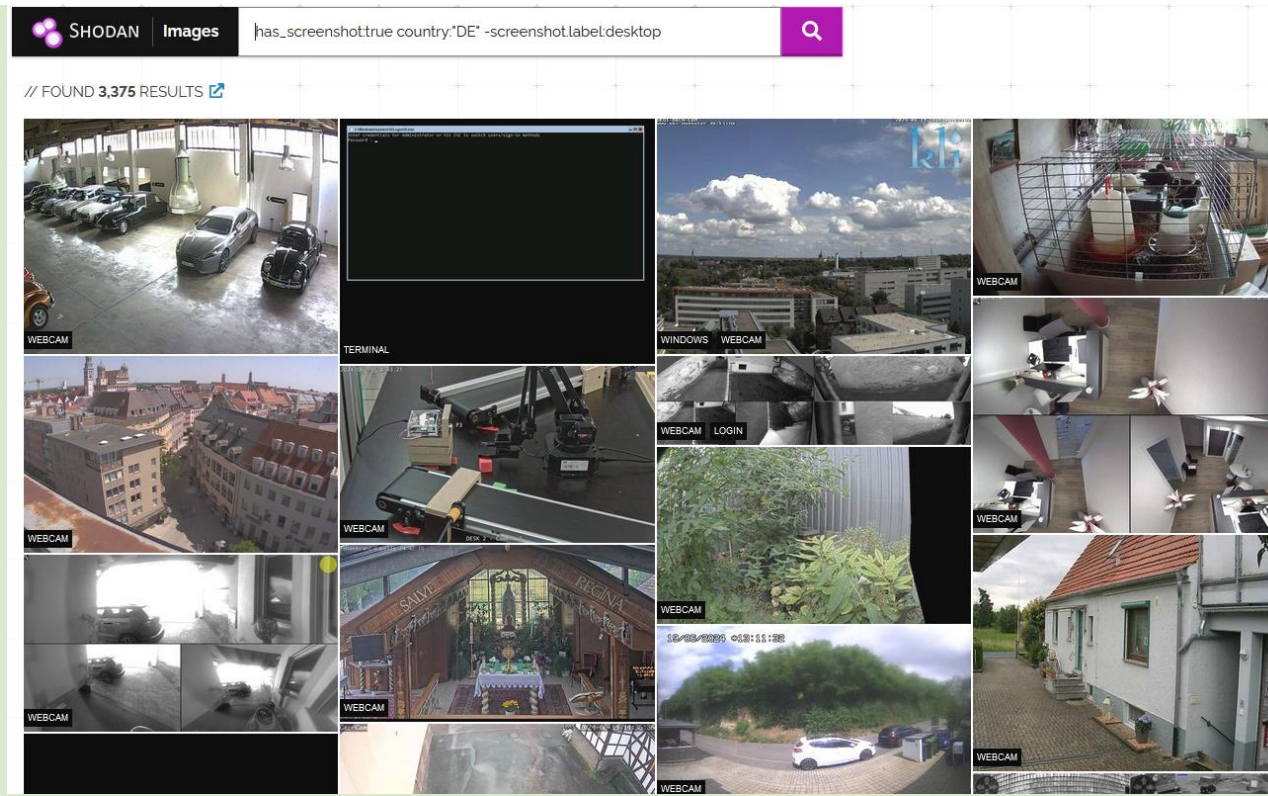
Portugal
Shodan.io - Search Engine for Internet Of Things

Logged In Remote Access

Germany
Shodan.io - Search Engine for Internet Of Things

THANK YOU

Q&A