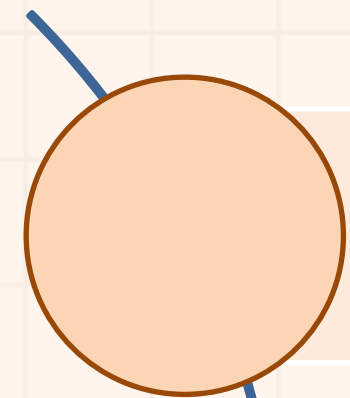




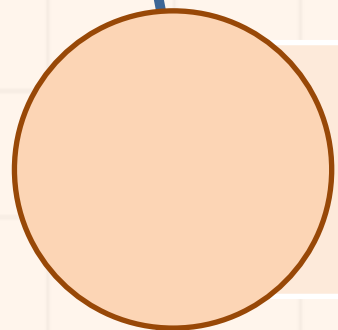
XC Safety-Security-Reliability Academy 2025

03/06/2025

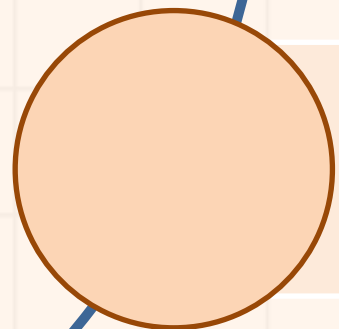
Agenda



Vulnerability

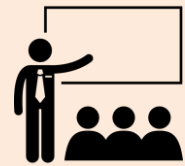


Common Attack Vectors



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 not related to my work or employer.

images: Flaticon.com



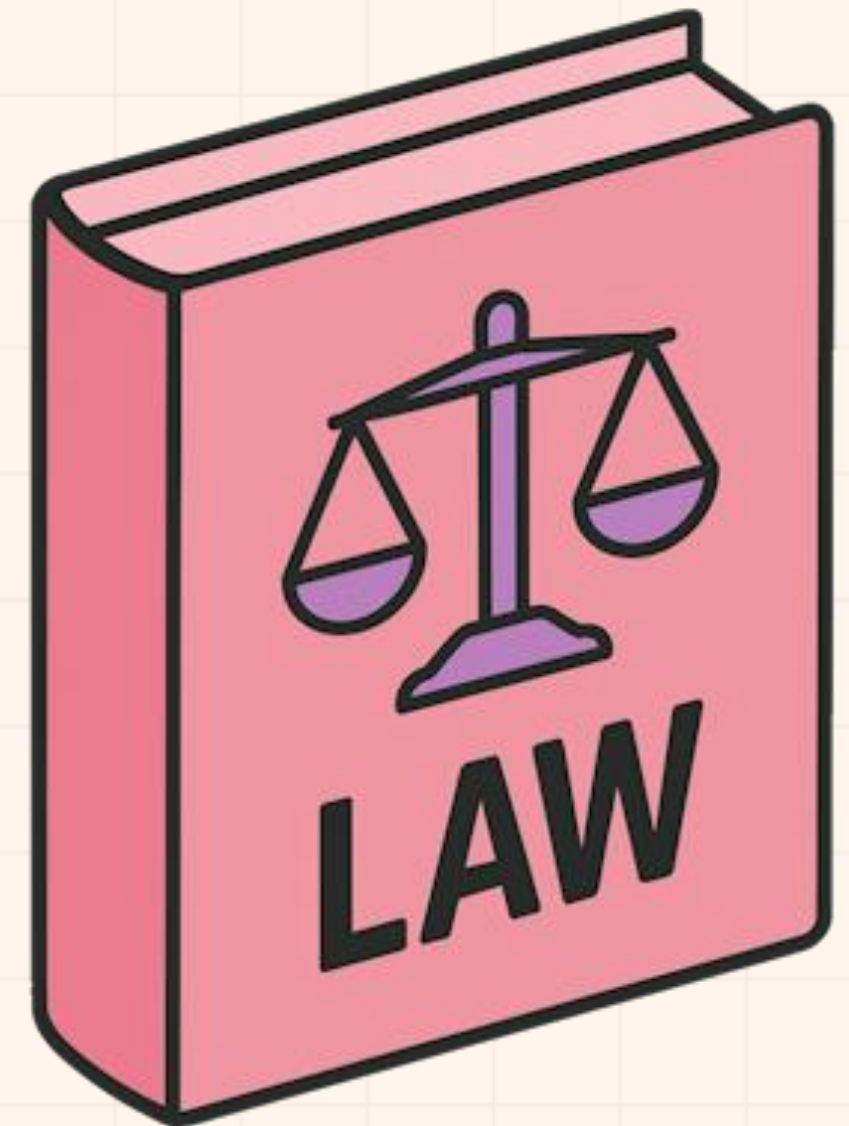
Disclaimer & Legal Considerations

German Law

- Bundesgesetzblatt ([link](#))
- Bundesnetzagentur ([link](#))

Organizations

- BSI – Bundesamt für Sicherheit in der Informationstechnik ([link](#))
- Incident Reporting ([link](#))
- CERT-Bund ([link](#))
- Bundeskriminalamt ([link](#))
- Generalstaatsanwaltschaft ([link](#))



Disclaimer & Legal Considerations

ARTIFICIAL INTELLIGENCE

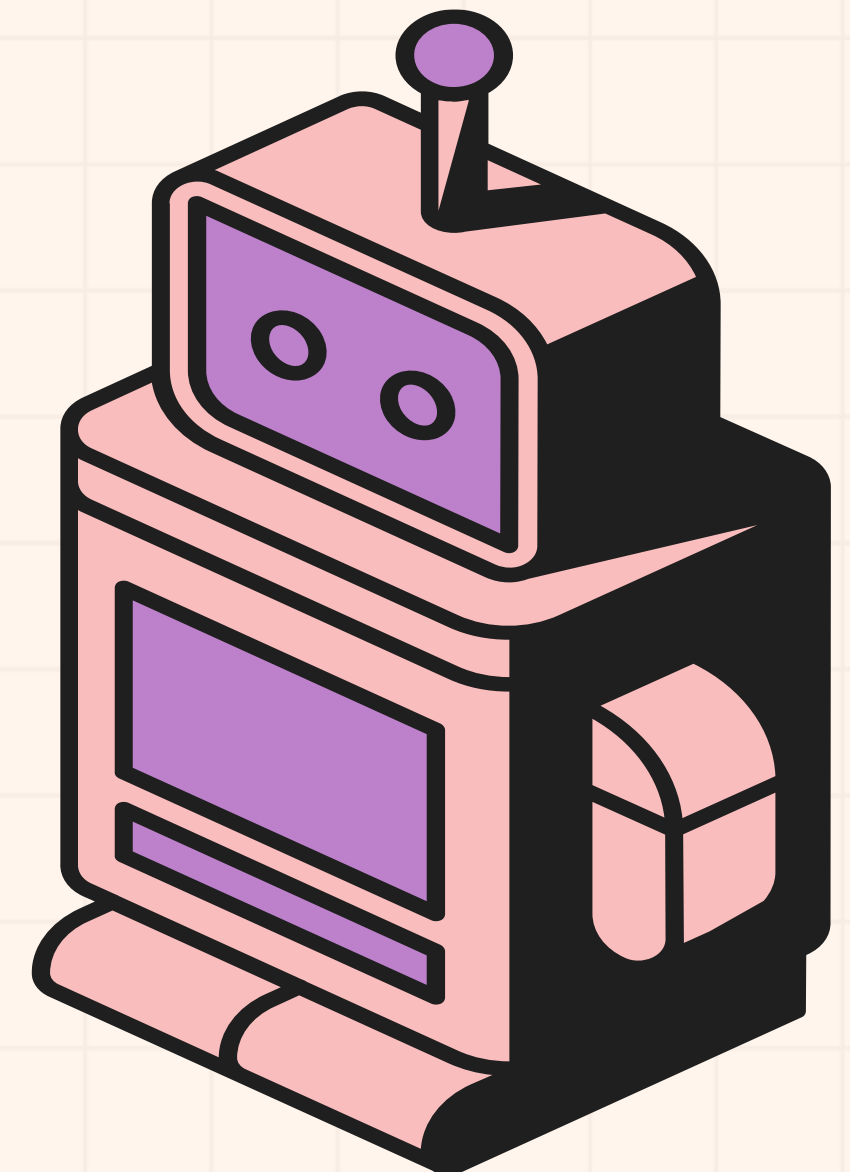
Was heavily used for this presentation

Use available technologies but check facts.

Always check facts.

AI is more than ChatGPT. Grok, Claude, ...

Use them all.



\$whoami

🕶️ Pedro Vieira

🔒 Cybersecurity Engineer

🕵️ OSINT

🖋️ Full stack developer

👤 Public Speaker



Vulnerability

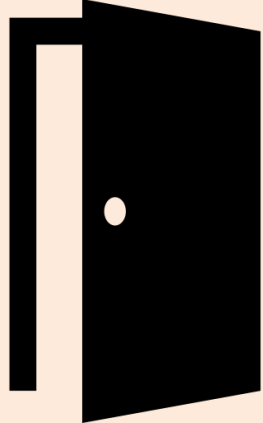

Definition and Statistics

Vulnerability - Vulnerability vs incident

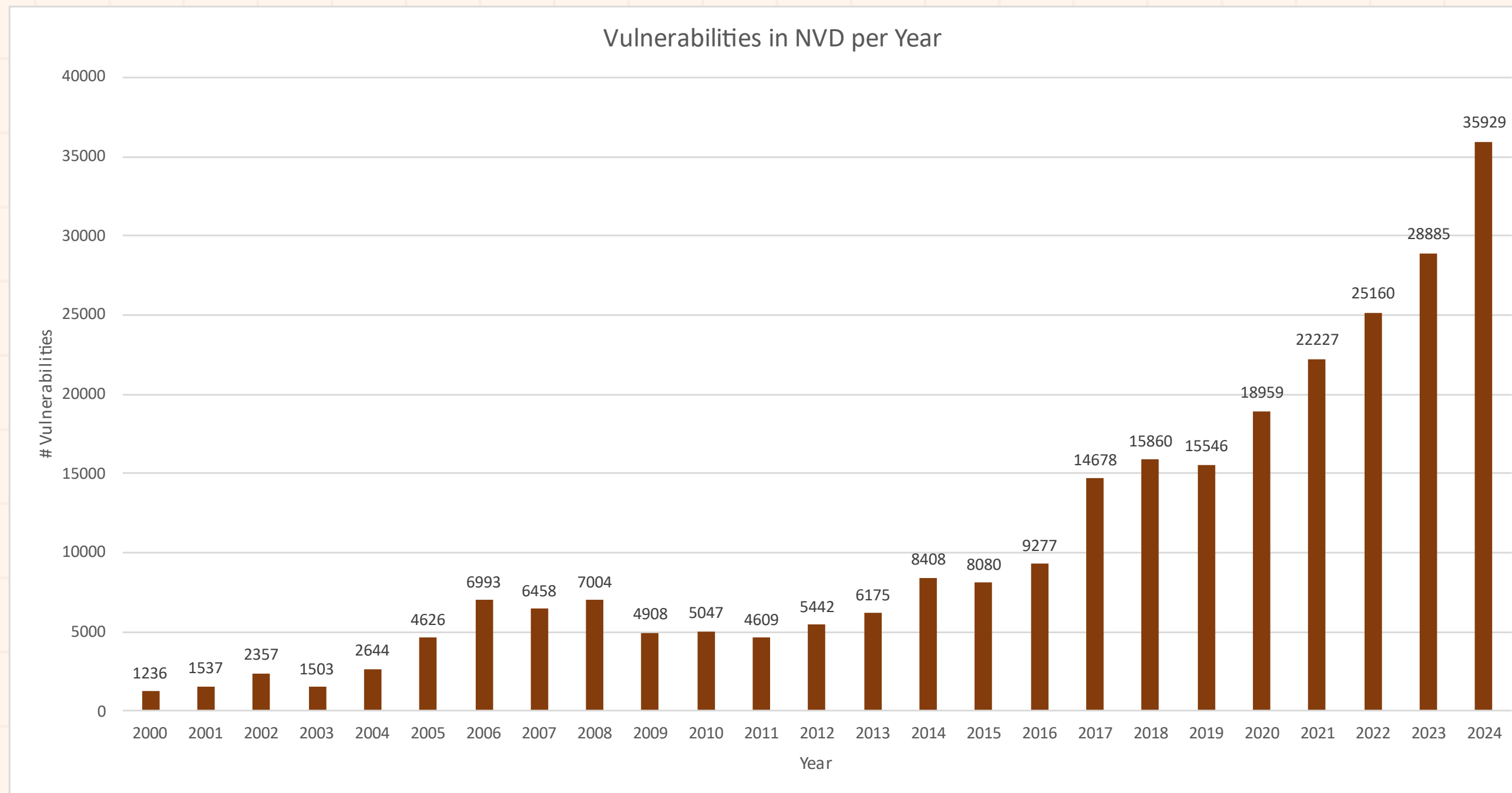
Logged In Remote Access

"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 

Vulnerability - Statistics by Year

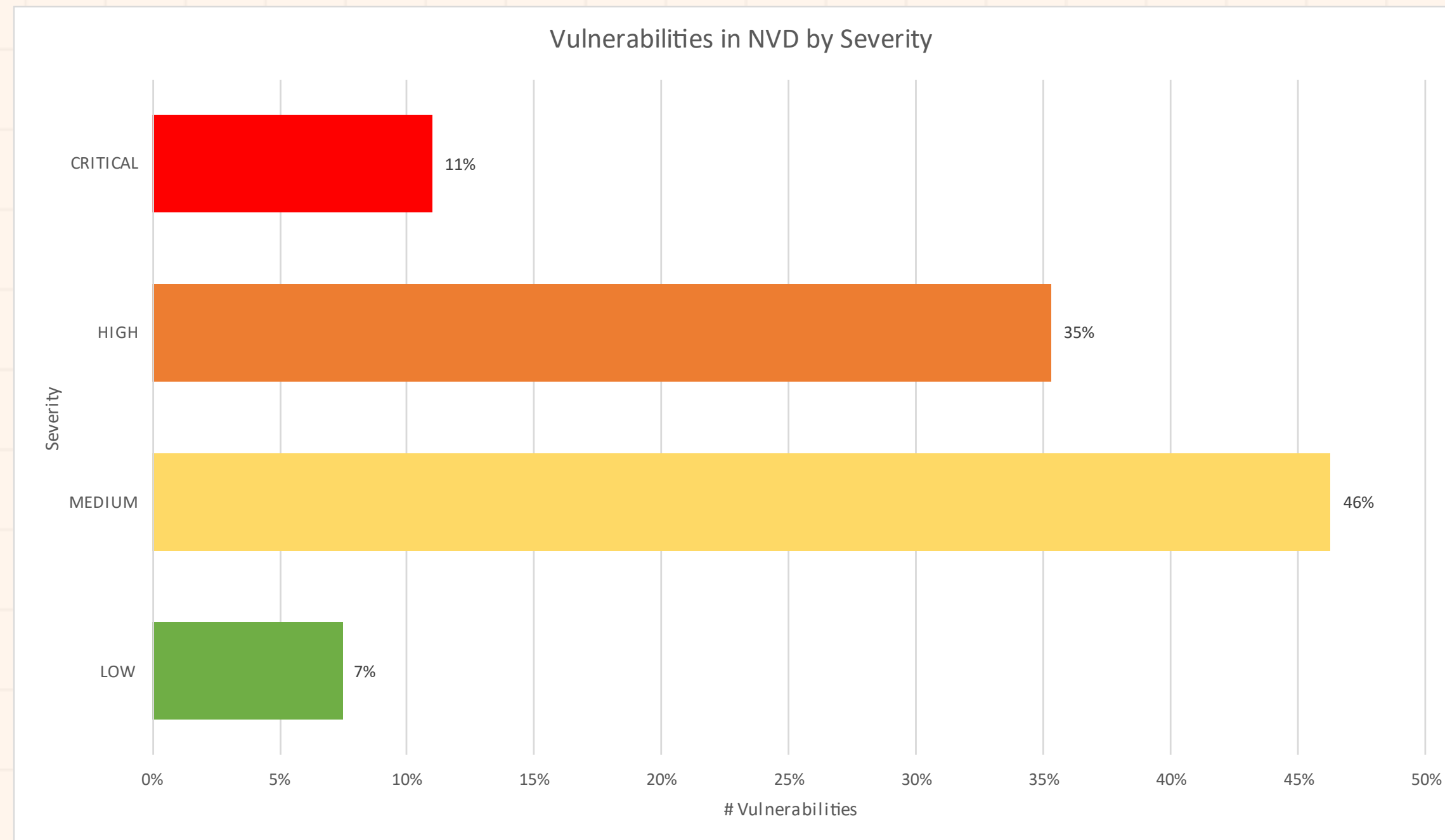


**Total known
vulnerabilities**

263.548

Source NVD 29/05/2025

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

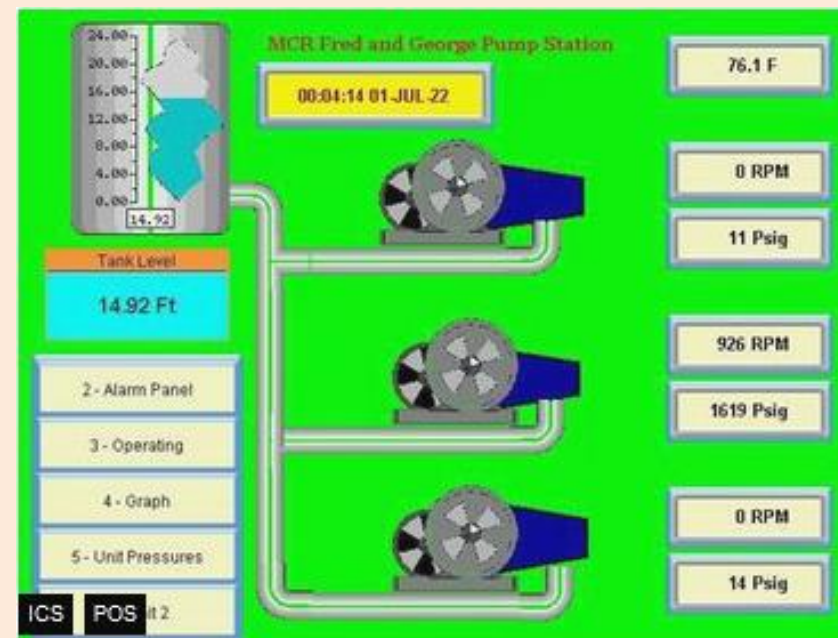
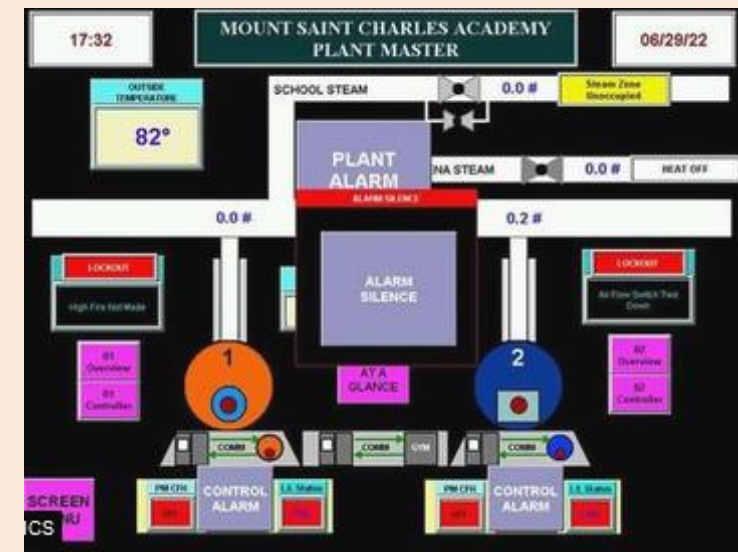
Source NVD 29/05/2025

Vulnerability - Examples from Shodan.io

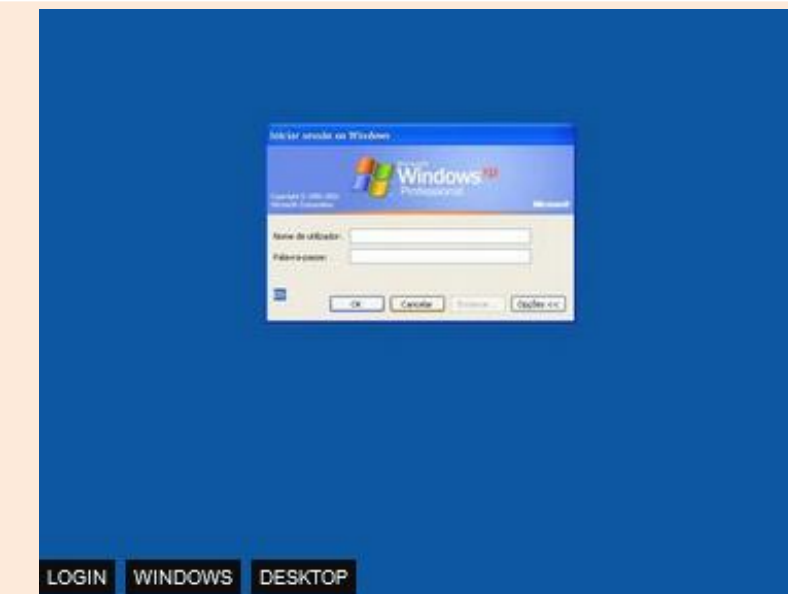
Default/No Password



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:

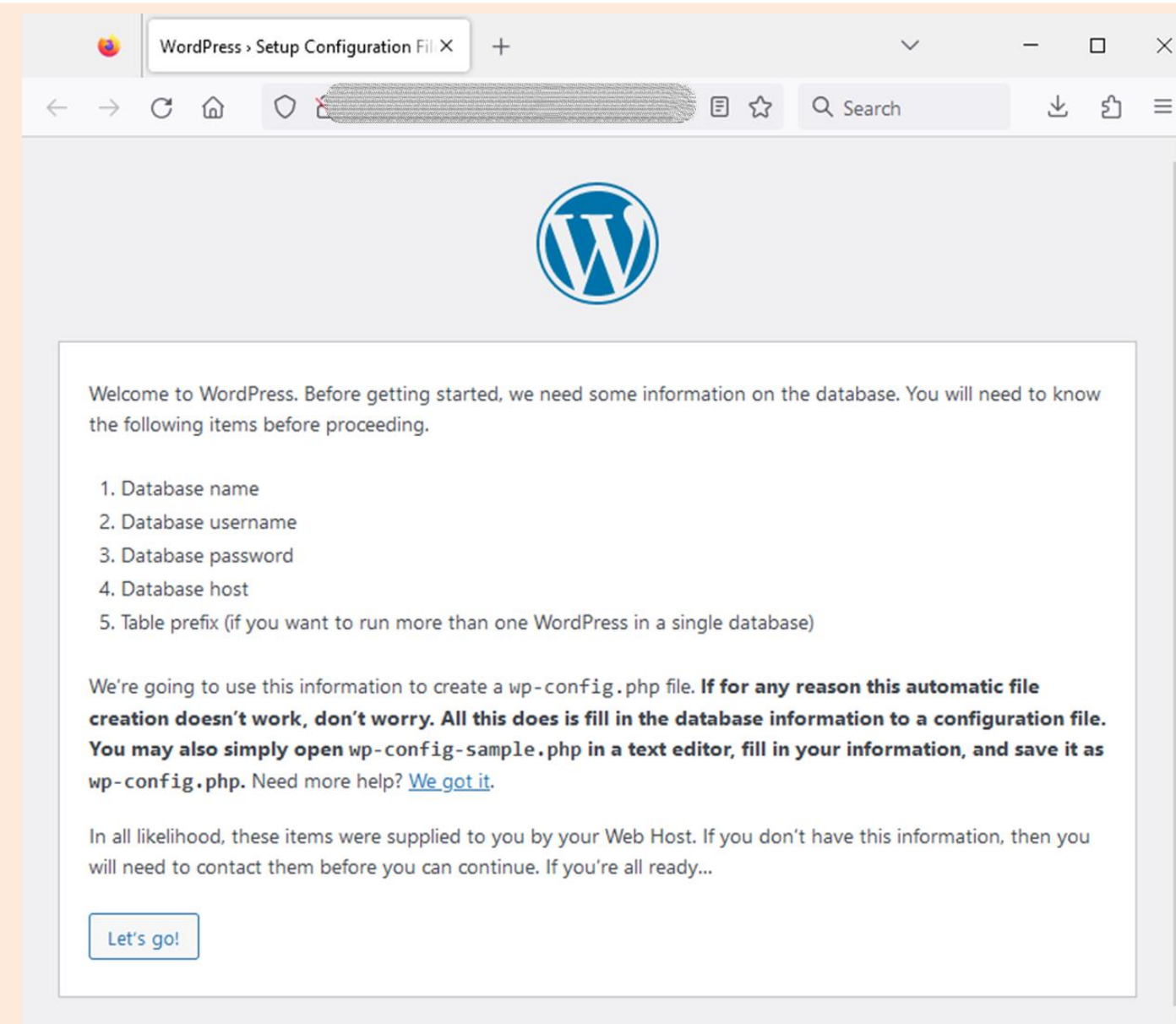
Authentication:	disabled
SMB Version:	2
Capabilities:	raw-mode

Shares		
Name	Type	Comments

Multimedia	Disk	System default share
Download	Disk	System default share
Recordings	Disk	System default share
Web	Disk	System default share
Public	Disk	System default share
homes	Disk	System default share
immogekko	Disk	
gerlinde	Disk	
SCAN	Disk	
admin	Disk	
HOB	Disk	
Buchhaltung	Disk	
Backup	Disk	Server, 3CX
home	Disk	Home
Haus&Co	Disk	Haus & Co Immobilienreuehand GmbH
IPC\$	IPC	IPC Service (NAS Server)

Accounting

WordPress site – Configuration available



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 UM 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><p>Redeemer Ransomware - Your Data Is Encrypted</p><p>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</p><p>Made by Cerebrate Visit the official Redeemer Ransomware Tor website - redeemergd6gjtzgjuif5jgpkk6i3xybkhsldzjoyjaxivyZlnhvmzcad.onion</p><p>[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.</p><p>[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).</p><p>[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.</p><p>OK</p></div>	<div><p>summary</p><p>may 29th, 2025</p><p>ransomwatch is currently crawling 492 sites belonging to 216 unique groups</p><p>🕒 there have been 6 posts within the last 24 hours</p><p>👤 there have been 160 posts within the month of may</p><p>📅 there have been 685 posts within the last 90 days</p><p>📁 there have been 1384 posts within the year of 2025</p><p>⚙️ there are currently 100 online hosts & 140 custom parsers.</p><p>🐛 ransomwatch has been running for 3 years, 8 months and 23 days and indexed 16015 posts</p><p>all data (<u>groups</u>) and (<u>posts</u>) is available in JSON (updated hourly)</p></div>

Common Attack Vectors - Malware - Ransomware

Ransomwatch

 recent posts

last 200 posts

date	title	group
2025-05-29	http://metromont.com	blacksuit
2025-05-29	Mulia Raya	ransomblog_noname
2025-05-28	KDV Label	play.
2025-05-28	Eliei Cycling	play.
2025-05-28	Cator Ruma & Associates	rhysida
2025-05-28	l*s.com.vn	flocker
2025-05-28	Fujipoly Ltd	spacebears
2025-05-27	Wrap & Send Services	hunters
2025-05-27	Eight8Ate Holdings, Inc	hunters
2025-05-27	http://www.iptelecom.at	ciphbit
2025-05-27	Corantioquia	hunters
2025-05-27	WAT Supplies	play.
2025-05-26	Media Links	play.

NoMoreRansom

<🔒/> NO MORE RANSOM

NEED HELP

unlocking your digital
life without paying
your attackers*?

YES

NO

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

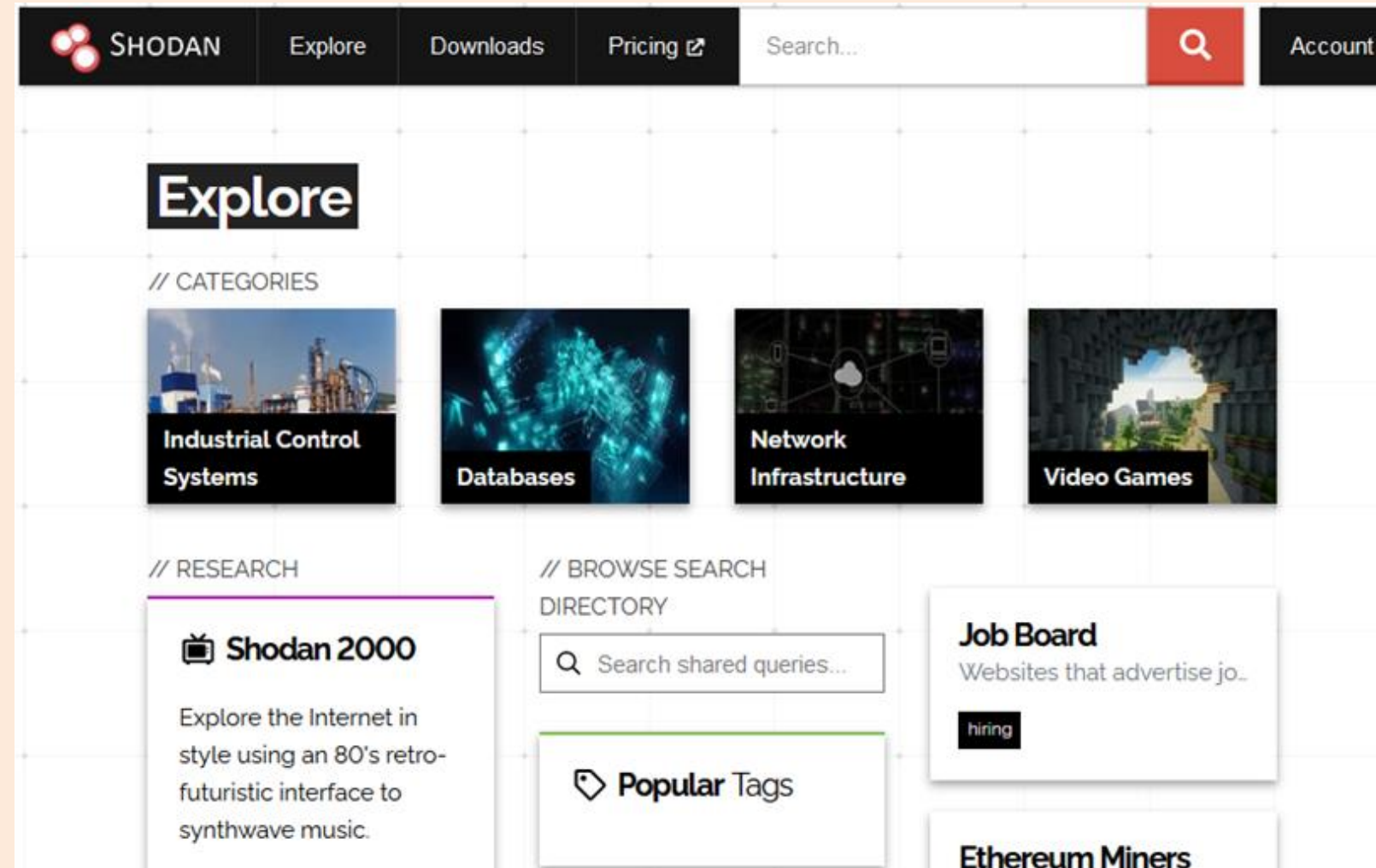
Page 17

German landscape

Definition and Statistics

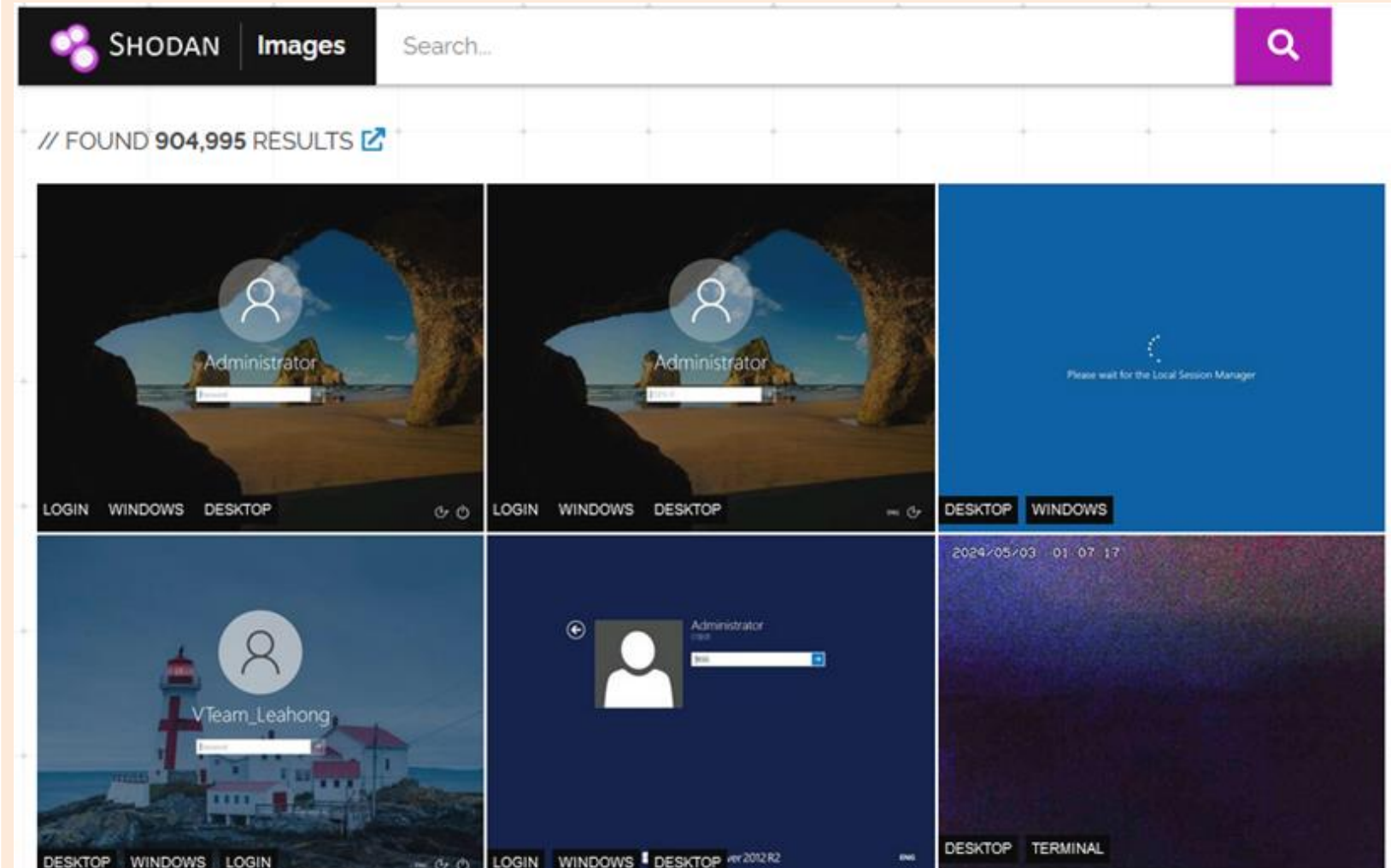
Germany - Shodan.io - Search Engine for Internet Of Things

Explore



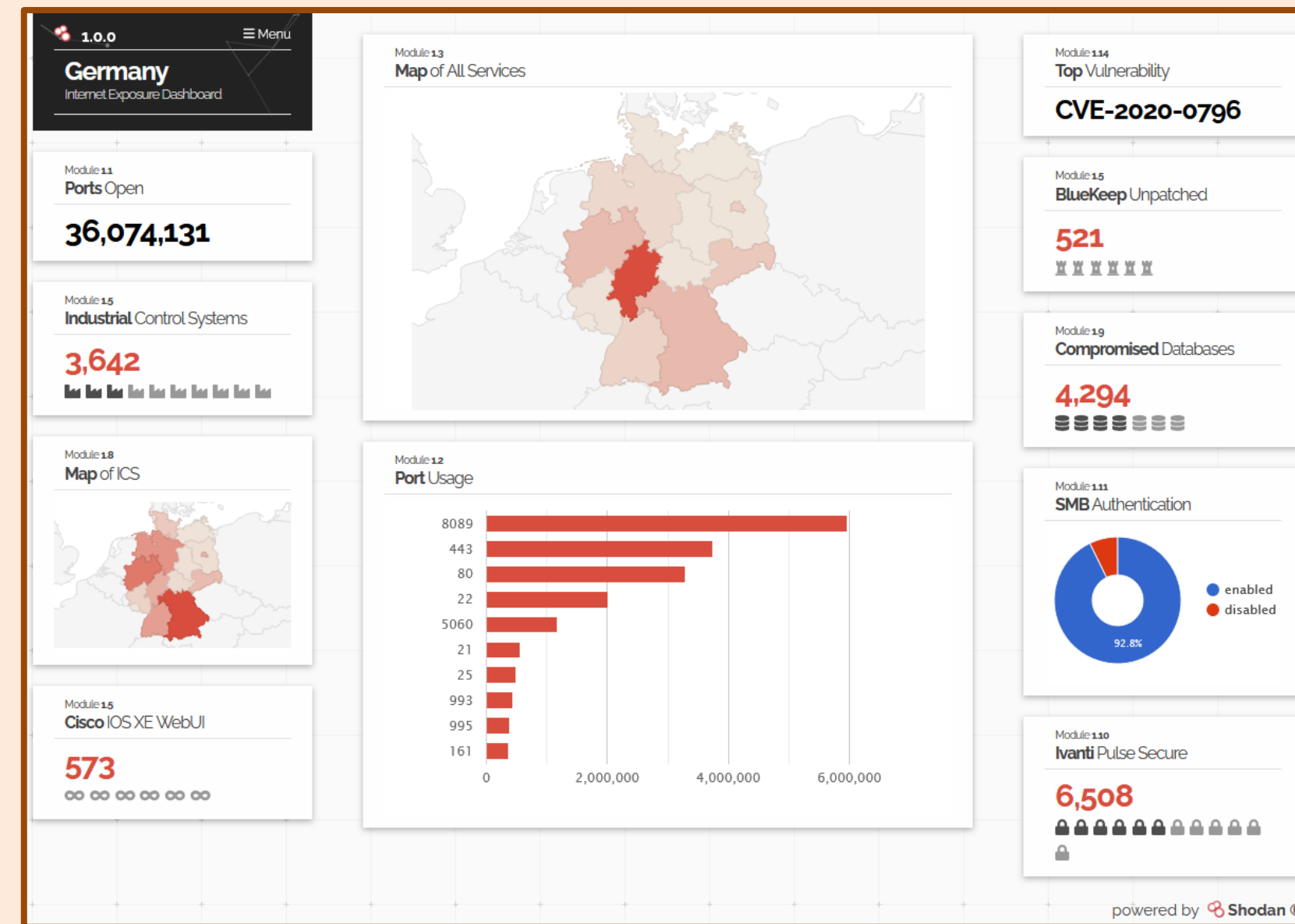
Shodan Queries ([link](#))

Images



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

Internet Exposure Observatory



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

Top in Germany - 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 3.11 (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

27,260

TOP CITIES

Berlin	8,991
Frankfurt am Main	6,750
Falkenstein	4,562
Düsseldorf	2,746
Nürnberg	1,558

[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

211

TOP CITIES

Nürnberg	89
Frankfurt am Main	52
Falkenstein	33
Berlin	6
Düsseldorf	4

[More...](#)

Germany - 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

3,346

TOP CITIES

Frankfurt am Main	699
Falkenstein	633
Berlin	462
Stuttgart	292
Dresden	165

[More...](#)

Logjam - CVE-2022-32548

⚠ Vulnerabilities

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

TOTAL RESULTS

2,143

TOP CITIES

Berlin	156
Hamburg	105
Frankfurt am Main	68
Munich	55
Köln	48

[More...](#)

Germany - 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'.

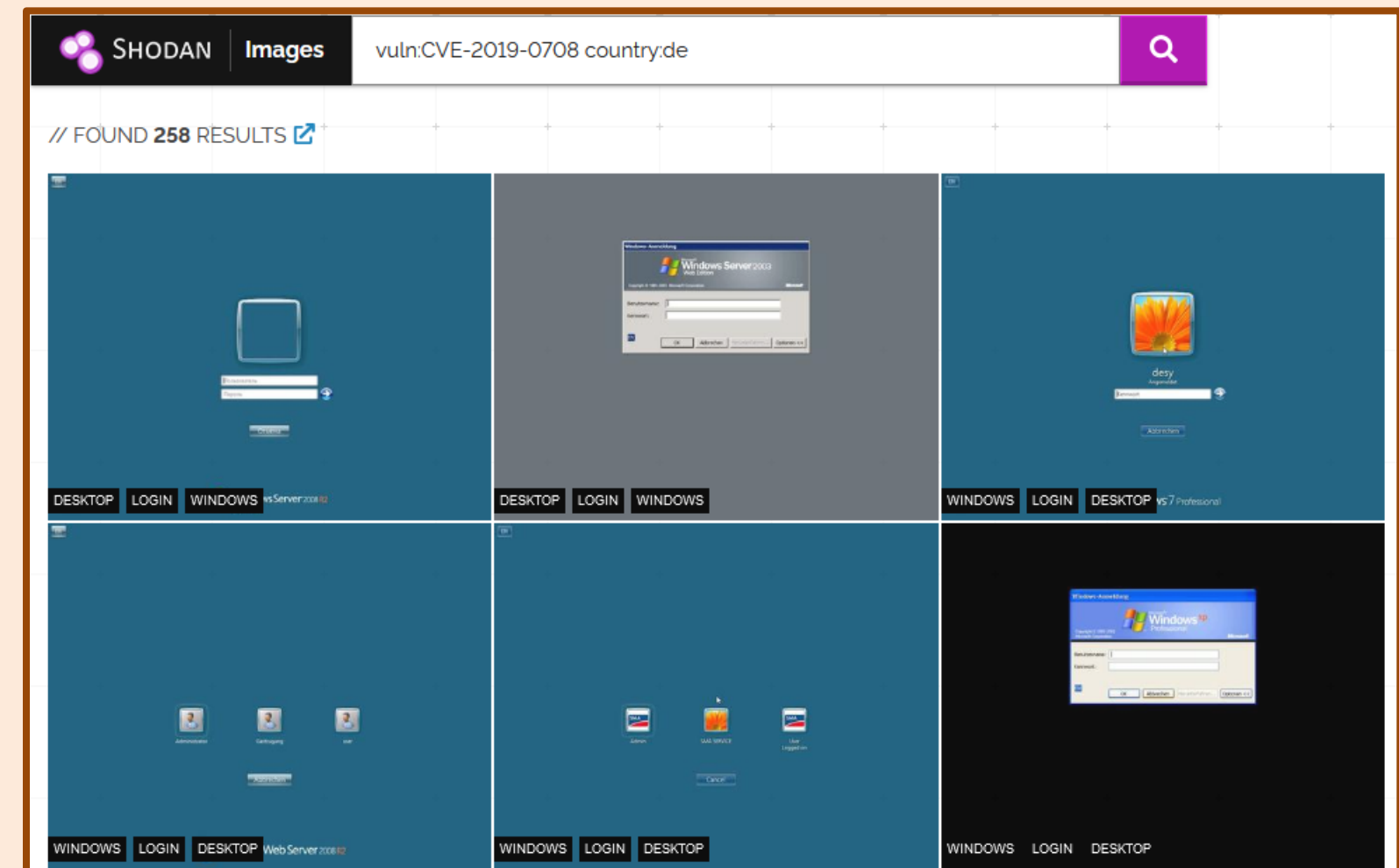
TOTAL RESULTS

552

TOP CITIES

Frankfurt am Main	147
Berlin	88
Falkenstein	40
Düsseldorf	33
Dresden	26

[More...](#)



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

Shared Folders

TOTAL RESULTS

4,522

TOP CITIES

Frankfurt am Main	1,566
Falkenstein	743
Nürnberg	473
Düsseldorf	406
Berlin	375

[More...](#)

SMB Status:

Authentication: disabled

SMB Version: 2

Capabilities: raw-mode

Shares

Name	Type	Comments
profiles	Disk	Network Profile
users	Disk	All users
groups	Disk	All groups
print\$	Disk	Printer Drive
service-update	Disk	Temp
prog	Disk	Diehl Program
GDL4-DATEN	Disk	GDL4-DATEN
GDL4-CRM	Disk	GDL4-CRM
DEMO-DV-IMPORT	Disk	DEMO-DV-IMPORT
DEMO-DV-EXPORT	Disk	DEMO-DV-EXPORT
RDL3-CRM	Disk	RDL3-CRM
RDL3-DATEN	Disk	RDL3-DATEN
IPC\$	IPC	IPC Service (Samba 4.21.3-git.385.dab56
nobody	Disk	Home Directories

Shares

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

Shares

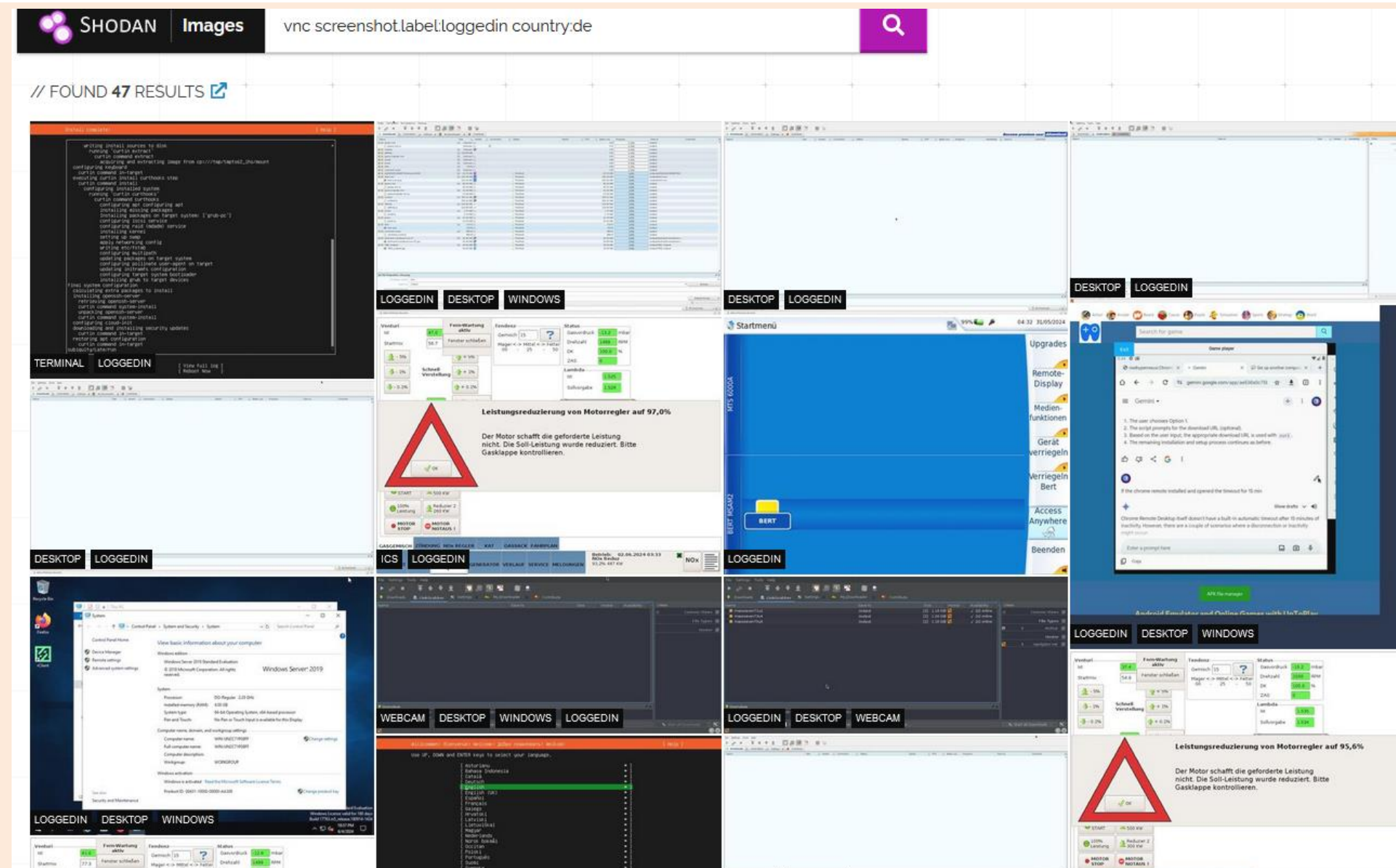
Name	Type	Comments
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC

Shares

Name	Type	Comments
logs	Disk	The recieved log files from customers.
IPC\$	IPC	IPC Service (Ubuntu-1804-bionic-64-minimal server (Samba, Ubuntu))

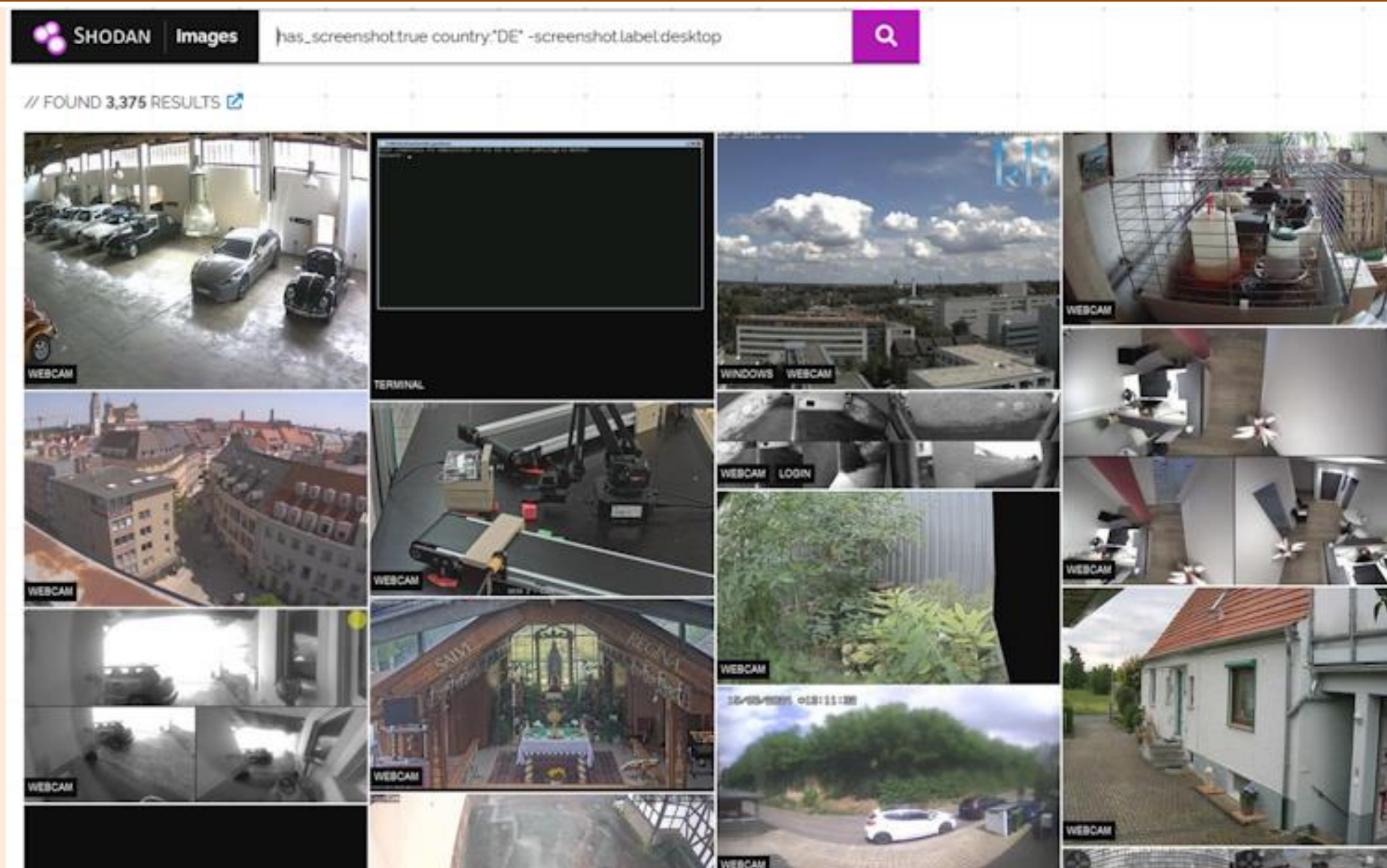
Germany - Shodan.io - Search Engine for Internet Of Things

Logged In Remote Access



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

Webcam



THANK YOU

Q & A

