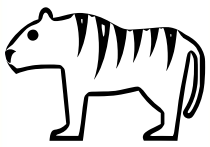
PrivacyWeek
2k18
25.10.2018

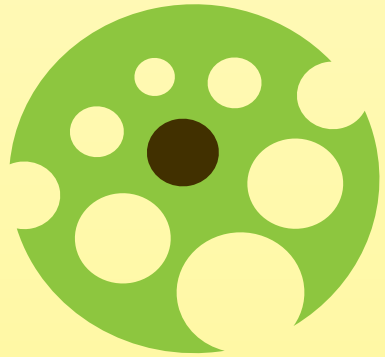
Security Safari in b0rkenLand

Hetti



Disclaimer

In diesem Vortrag geht es (noch immer)
nicht um den Safari Browser



National 

Security Awareness Month

Informationssicherheit

3 Grundpfeiler
+
Neuland
=
R e a l i t ä t

C I A

Grundpfeiler

C onfidentiality - Vertraulicheit

I ntegrity - Integrität

A vailability - Verfügbarkeit

Security 101

DoS

Command Injection

Auth Bypass

Backdoor

CVE

RCE

CVSS

PoC

CVE

Common Vulnerabilities and Exposures

- Beispiel: CVE-2017-0143

CVSS

Common Vulnerability Scoring System

- Scoring: 0-10

Command Injection

Selbst kontrollierbare Kommandos in ein System injizieren.

Kategorie:

Einfach nur fail!

NPM – 5.7.0 "release

- Hat alle Rechte "random" geändert
- Mit sudo aufgerufen: Ändert Rechte von Ordnern rekursiv
- Das release war nicht korrekt gekennzeichnet als pre release
- CVE-2018-7408

juggy commented on Feb 22

This destroyed 3 production server after a single deploy!

👍 61	👎 13	😄 72	🎉 330	😕 58	❤️ 26

https://github.com/npm/npm/issues/19883#issuecomment-367570304

pakastin commented on Feb 22

Why are you using a pre-release version in production **@juggy**? Just asking...

👍 58	👎 83	😄 15	🎉 9	😕 11

https://github.com/npm/npm/issues/19883#issuecomment-367642094

Windows 10 Update (Version 1809)

- Windows 10 Update Anfang Oktober
- Löschte Dateien in «Eigene Dateien» Ordner unter bestimmten Umständen
- Wurde mittlerweile von Micosoft zurückgezogen

Backdoor

Eingebaute Methode um Authentifizierung || Verschlüsselung zu umgehen von einem System

Cisco Backdoors

- hat lange Backdoor Historie
- Positiv: Interne Auditierung !
- Sehr kreativ im Synonyme erfinden

Cisco Backdoors

- Beispiele:

"undocumented user account with privilege level 15"
CVE-2018-0150

"undocumented, static user credentials for the default administrative account"
CVE-2018-0222

"undocumented test interface"
CVE-2014-0659

Tenda AC15 Backdoor

- Internet WiFi Router

- Adminzugang in 3 leichten Schritten

1) /goform/telnet aufrufen → startet telnet
2) Freie Wahl aus 3 existierenden Standard Accounts am Gerät die Admins sind
Password? Ratet!
1234
3) login → protifitieren

- CVE-2018-5770


THE NINETIES CALLED
THEY WANT THEIR PASSWORDS BACK
imgflip.com

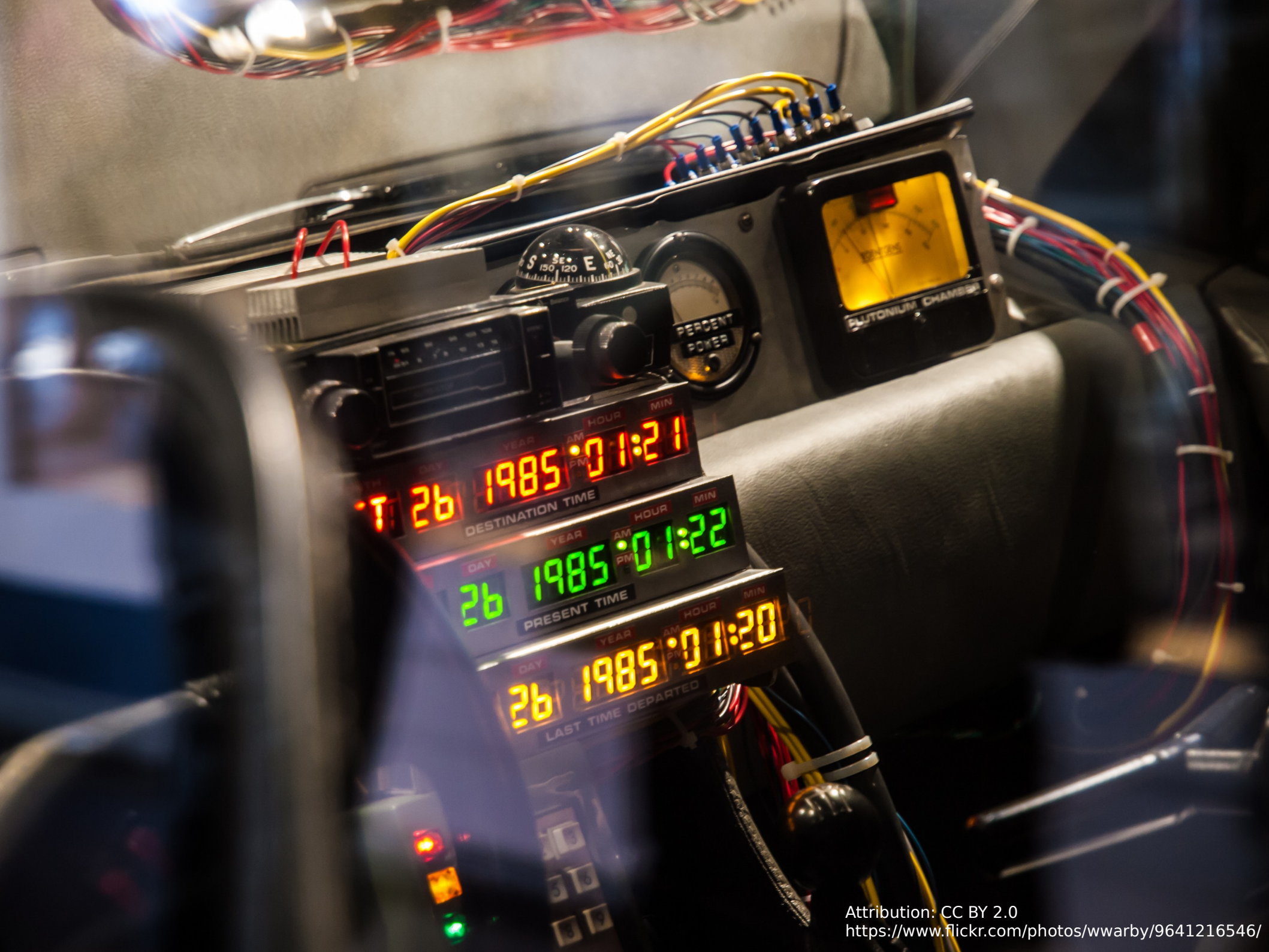
Auth Bypass

Umgehung der Authentifizierung

Blast from the past!

Netscape gained privileges

- Netscape Enterprise Server & Netscape FastTrack Server
- Remote Attacke
- Rechte bekommen via HTTP Basic Auth
- CVE-1999-0853

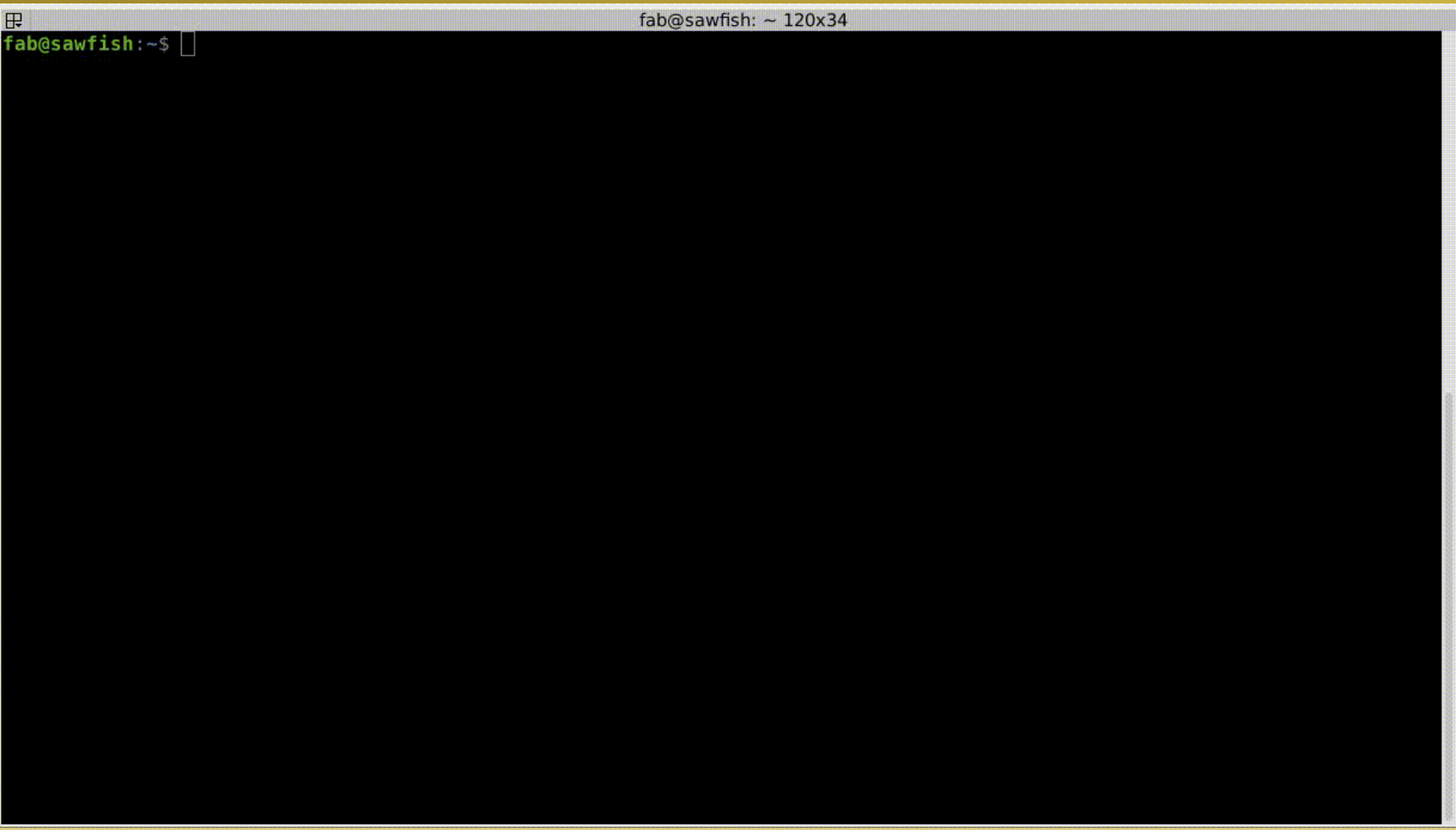


Back to the future!

HPE iLO4 Auth Bypass + RCE

- remote management console für Server
- Authentification bypass + RCE
- von 2017, öffentlich bekannt in 2018 - CVE-2017-12542

HPE iLO4 Auth Bypass



Source: https://github.com/airbus-seclab/ilo4_toolbox

1999 = 2018

BUFFER OVERFLOW

Datenreichtum

!Datensparsamkeit

Digitales Gold

unnötig

Google Plus Datenleak

- ca. 500.000 Benutzer betroffen
- Teilweise sensible Daten entwendet
- Google Plus wurde eingestellt

Facebook Datenleak

💰 ca. ~~50.000.000~~ 30.000.000 Benutzer betroffen

💰 60x so viele Benutzer wie vom G+ Leak betroffen

💰 Sie haben noch nicht zugemacht

DoS

Denial of Service

Unterbrechung des Dienstes

Netwave IP Kamera - DoS

- POST Anfrage mit großer Body size zur / URI → Crasht die Kamera

- PoC auf Github
https://github.com/dreadlocked/netwave-dosvulnerability

- CVE-2018-6479

RCE

Remote Code Execution

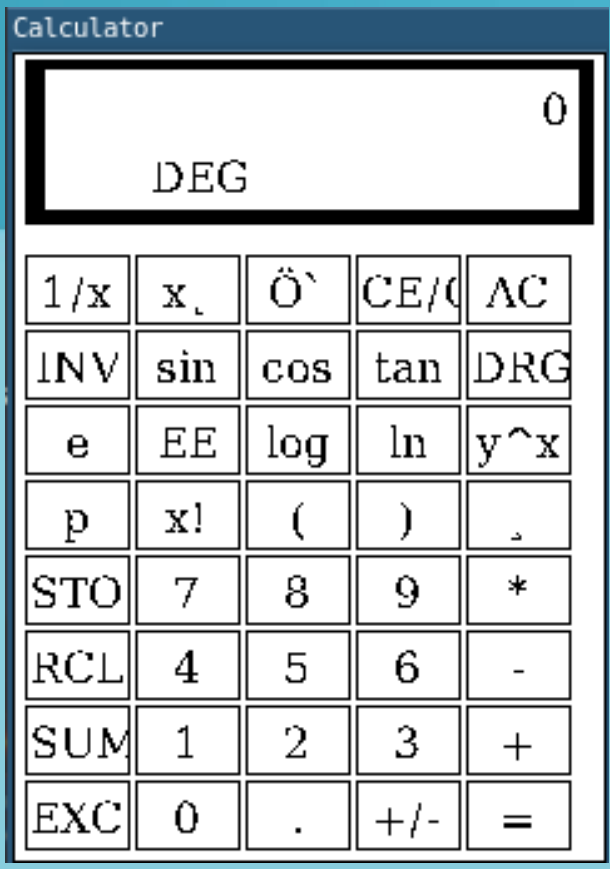
Eigenen Code/eigene Programme auf einem entfernten Ziel ausführen

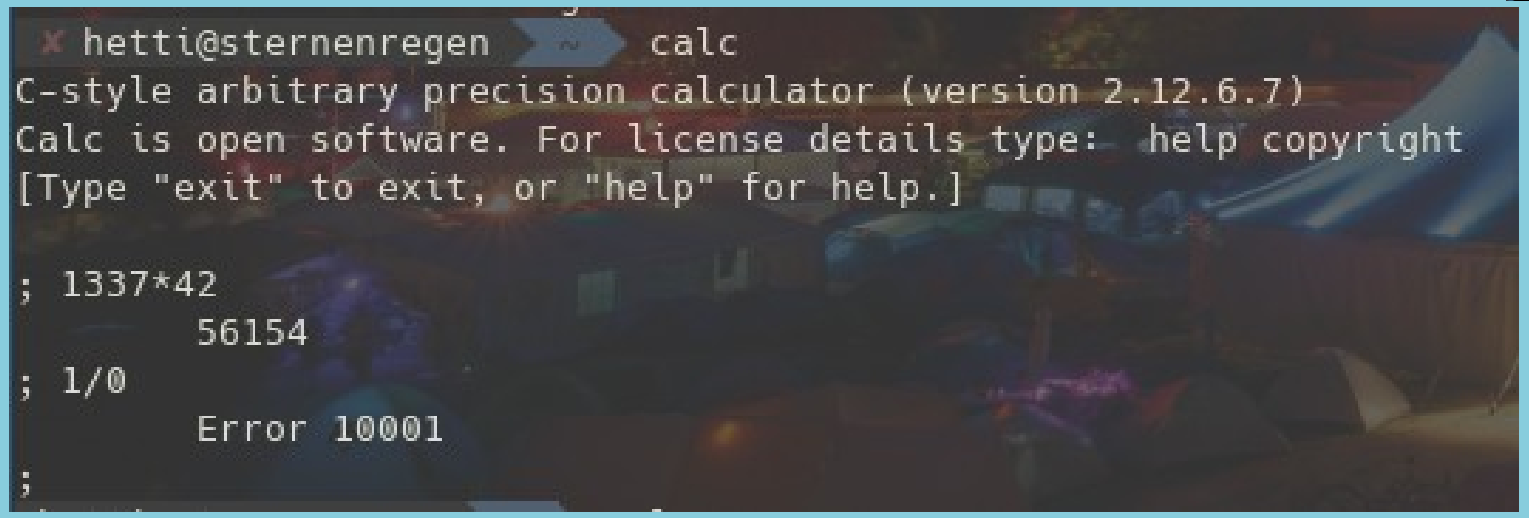
Steam RCE

- existierte 10 Jahre im Client
- manipuliertes UDP Packet reicht um den Exploit zu triggern
- Ausführliche Zusammenfassung unter https://www.contextis.com/blog/frag-grenade-a-remote-code-execution-vulnerability-in-the-steam-client

PoC

Proof of Concept






HELLO
CAN I HAVE A LIVE DEMO?
imgflip.com


LIVE DEMO!
38
WHAT COULD POSSIBLY GO WRONG?
imgflip.com

Ghostscript RCE

- Übersehen, als vor 2 Jahren gepatch wurde
- Trigger: z.B. verarbeiten von Postscript
- Gefunden durch Tavis Ormadi

Diskussion auf der ML:
https://seclists.org/oss-sec/2018/q3/157

- Mehrere CVEs zugewiesen

Exploit chain!

Thanks Lena for the Meme :-)


WTF
JUST HAPPENED
imgflip.com

Exploitchain Recap

Downloading 4K "CatPictures" :`D
+ öffnen in Nautilus

↓

Ghostscript RCE

↓

Virtualbox Ausbruch zum Host System

↓

Root am Host via DirtyCow

Setup

Host System: Ubuntu 16.04.4 – unpatched

VirtualBox 5.2.6.r120293

Guest System: Debian 9 mit GUI
– halbwegs gepatcht

Guest Benutzer hat sudo mit NOPW Option

Selbstgeschriebene Exploitchain
- Python
- Bash
- (modifizierte) verfügbare PoCs

VirtualBox VM Escape

VRAM benutzt für den Exploit

Shared Video Buffer (Host+Guest)

Exzellente Zusammenfassung vom PoC Author (ENG):
https://www.voidsecurity.in/2018/08/from-compiler-optimization-to-code.html

CVE-2018-2844

DirtyCow?

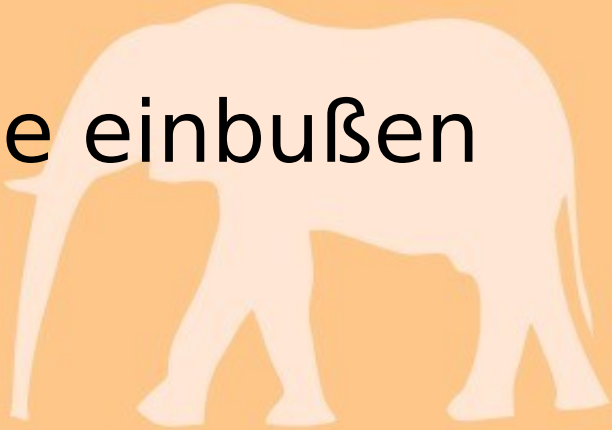
Hausaufgabe fürs Publikum

Tipp: CVE-2016-5195

Hardware Security

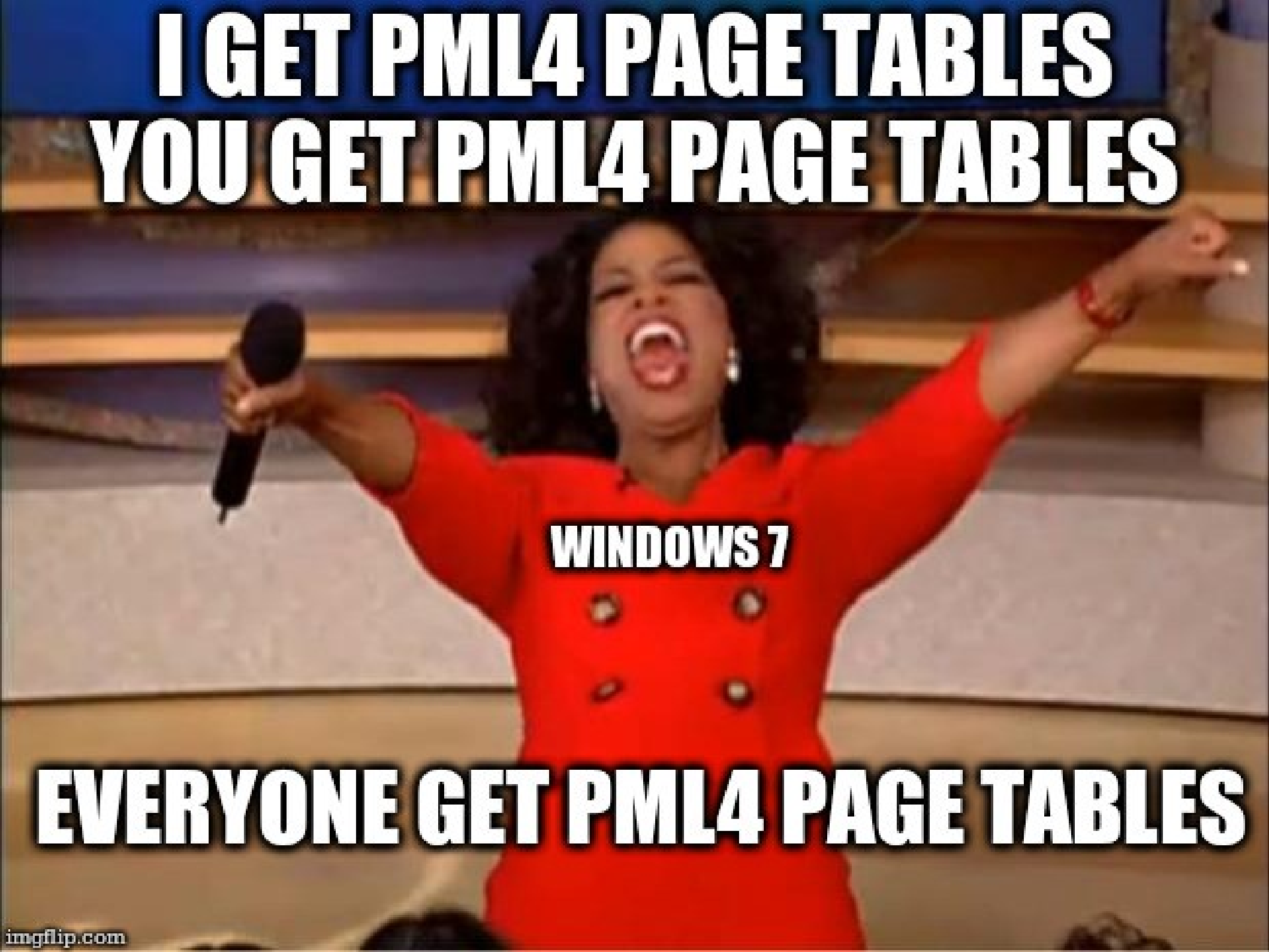
Meltdown && Spectre

- Führt zu Extraktion von sensiblen Daten
- Design Fehler in moderner CPU Architektur
- Hardware "bug" - Spekulative Exekution
- Software fixes → Performance einbußen



Meltdown "Patch"

- Patch für Win 7 & Win Server 2008 R2
- PLM4 Page Table zugreifbar für jeden
- Alle Programme hatten Vollzugriff
- «Patch» LOL


I GET PML4 PAGE TABLES
YOU GET PML4 PAGE TABLES
WINDOWS 7
EVERYONE GET PML4 PAGE TABLES
imgflip.com

BMW - Telematics Control Unit

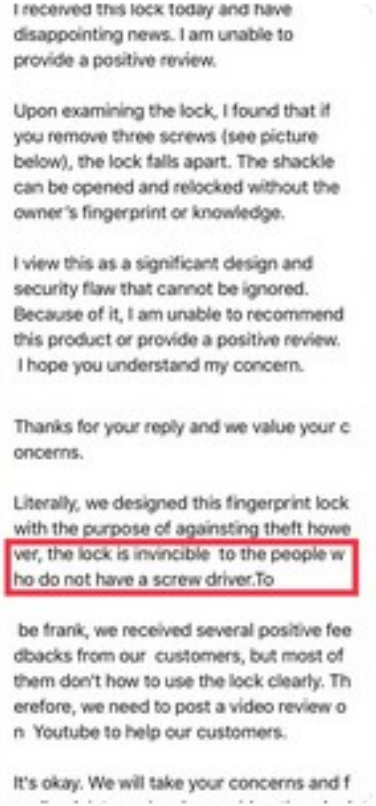
- BMW vehicles (2012 to 2018)
- remote attack
- execution (CAN bus) of arbitrary, unauthorized diagnostic requests
- CVE-2018-9318

LockPickingLawyer
@LockPickingLwyr

Folgen

The company that sent me the pictured fingerprint lock has provided the security quote of the year: “...the lock is invincible to the people who do not have a screwdriver.”

Tweet übersetzen



I received this lock today and have disappointing news. I am unable to provide a positive review.

Upon examining the lock, I found that if you remove three screws (see picture below), the lock falls apart. The shackle can be opened and relocked without the owner's fingerprint or knowledge.

I view this as a significant design and security flaw that cannot be ignored. Because of it, I am unable to recommend this product or provide a positive review. I hope you understand my concern.

Thanks for your reply and we value your c oncerns.

Literally, we designed this fingerprint lock with the purpose of againsting theft howe ver, the lock is invincible to the people w ho do not have a screw driver.To

be frank, we received several positive fee dbacks from our customers, but most of them don't how to use the lock clearly. Th erefore, we need to post a video review o n Youtube to help our customers.

It's okay. We will take your concerns and f

06:17 - 15. Juni 2018 aus Bethesda, MD

Kombiniert!

Mining Rigs

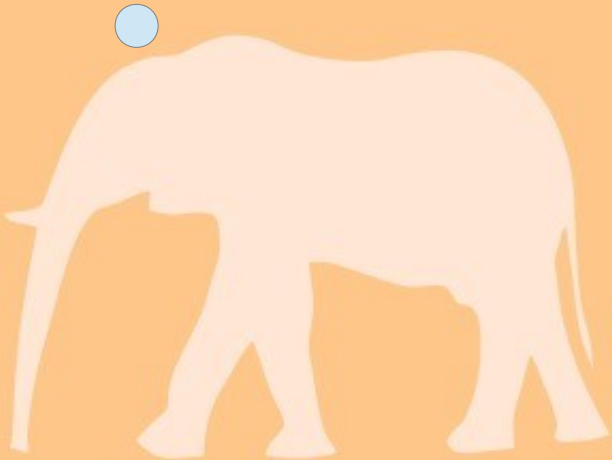
Datacenter

600

Island

Gestohlene Mining Rigs

Bitcoin heist: 600 powerful computers stolen in Iceland



Source:
https://www.apnews.com/55117fb55a714e909fb9aaf08841a5d6/Bitcoin-heist:-600-powerful-computers-stolen-in-Iceland

Gestohlene Mining Rigs

Gestohlene Mining Rigs
Bonus Content

'Big bitcoin heist' suspect escapes prison and flees Iceland 'on PM's plane'

Sindri Thor Stefansson escaped through window before reportedly boarding same flight to Sweden as prime minister Katrín Jakobsdóttir

Source:
https://www.theguardian.com/technology/2018/apr/18/big-bitcoin-heist-suspect-sindri-thor-stefansson-escapes-prison-flees-iceland-pm-katrin-jakobsdottir-plane

Sound + HDDs =

- Gas basiertes Feuerlösch System
- Festplatten zerstört
- Nicht genug Server in Schweden
- NASDAQ nicht operational

Shouting in the Datacenter: https://www.youtube.com/watch?v=tDacjrSCeq4
Source:
https://www.bleepingcomputer.com/news/technology/loud-sound-from-fire-alarm-system-shuts-down-nasdaqs-scandinavian-data-center/

Was geht
mich das an?

Security Probleme
betreffen uns alle
in irgendeiner Form!

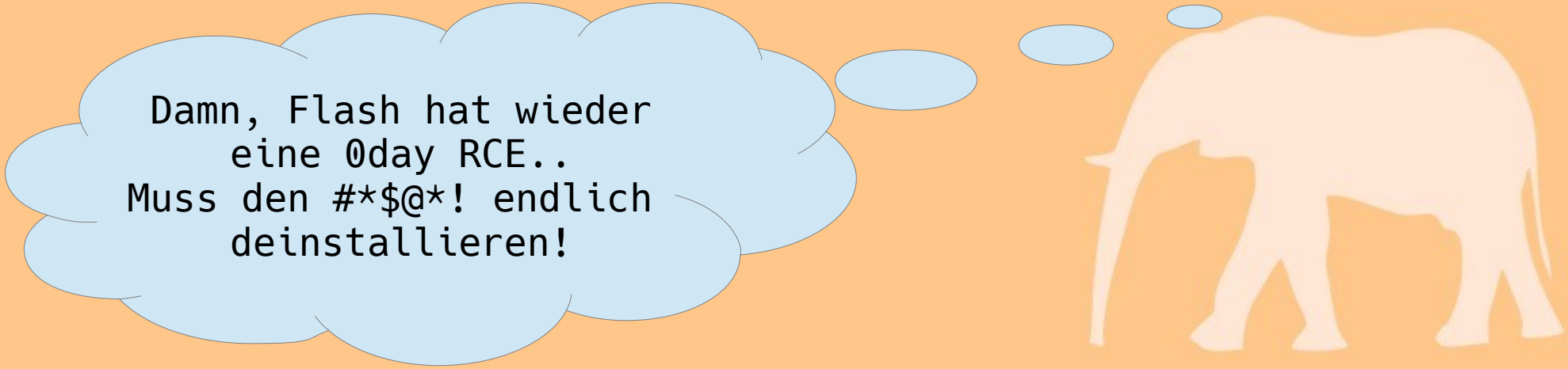
Macht die Welt zu einem sichereren Ort!

Get some Popcorn and take your time!

Interesse geweckt für den Security foo?
CVEs lesen ist lusting als auch interessant!

Wo bekommt man die CVE Details?

https://www.cvedetails.com/



FRAGEN?

Pr0ps go out to:

Family & Friends

All the folks that are working towards making the world a safer place

Reno Robert - @renorobertr
  For the VirtualBox PoC and support

Gbonacini – Github: gbonacini
  For the DirtyCow PoC

Tavis Ormandy - @taviso
  For the ghostscript PoC

DANKE SEHR!

BLEIBT SICHER
UND
PATCHT EURE SYSTEME!

CAN I HAE CONTACT?

Matrix: @hetti:matrix.org

Mastodon: @hetti@chaos.social

Github: https://github.com/hettipeti

Twitter: @Th3peko

Email: pw18@cyber.coffee