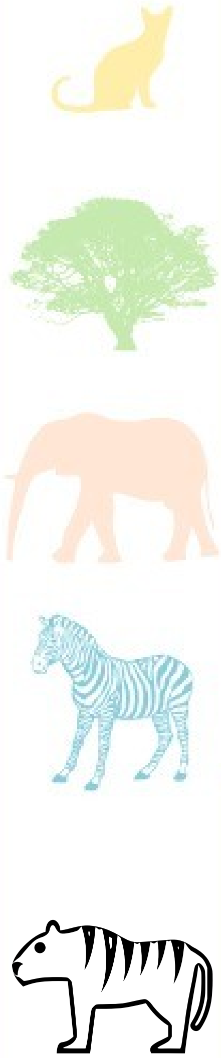
#35c3
2*.12.2*18



Security Expedition in b0rkenLand

Hetti

Information Security

3 fundamental aspects

+

Neuland

=

Reality

CIA

fundamental aspects

C onfidentiality

I ntegrity

A vailability

Security 101

DoS

Command Injection

Auth Bypass

Backdoor

CVE

RCE

CVSS

PoC

CVE

Common Vulnerabilities and Exposures

- Example: CVE–2017–0143

CVSS

Common Vulnerability Scoring System

- Scoring: 0-10

Command Injection

Inject own controlled commands into system

Category

Just Fail!

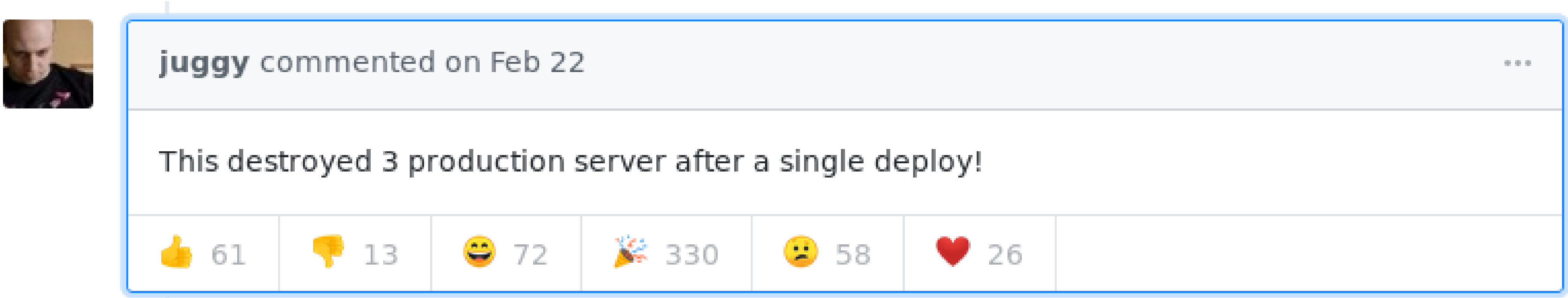
NPM – 5.7.0 "release"

Fucked up all permissions

running via sudo changed permissions recursivly on folders

the release was not properly tagged as pre release

CVE-2018-7408

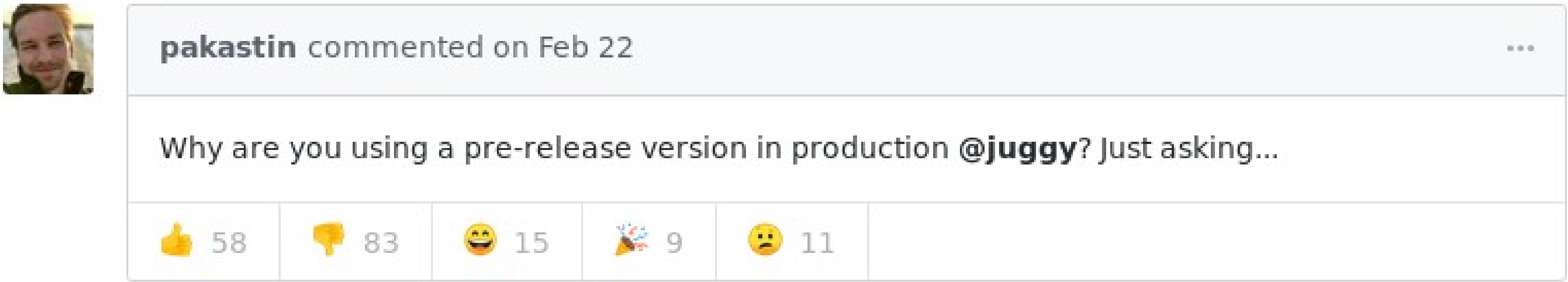


juggy commented on Feb 22

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

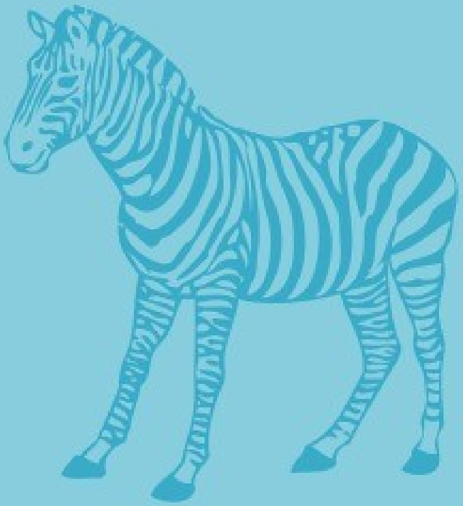
Why are you using a pre-release version in production **@juggy**? Just asking...

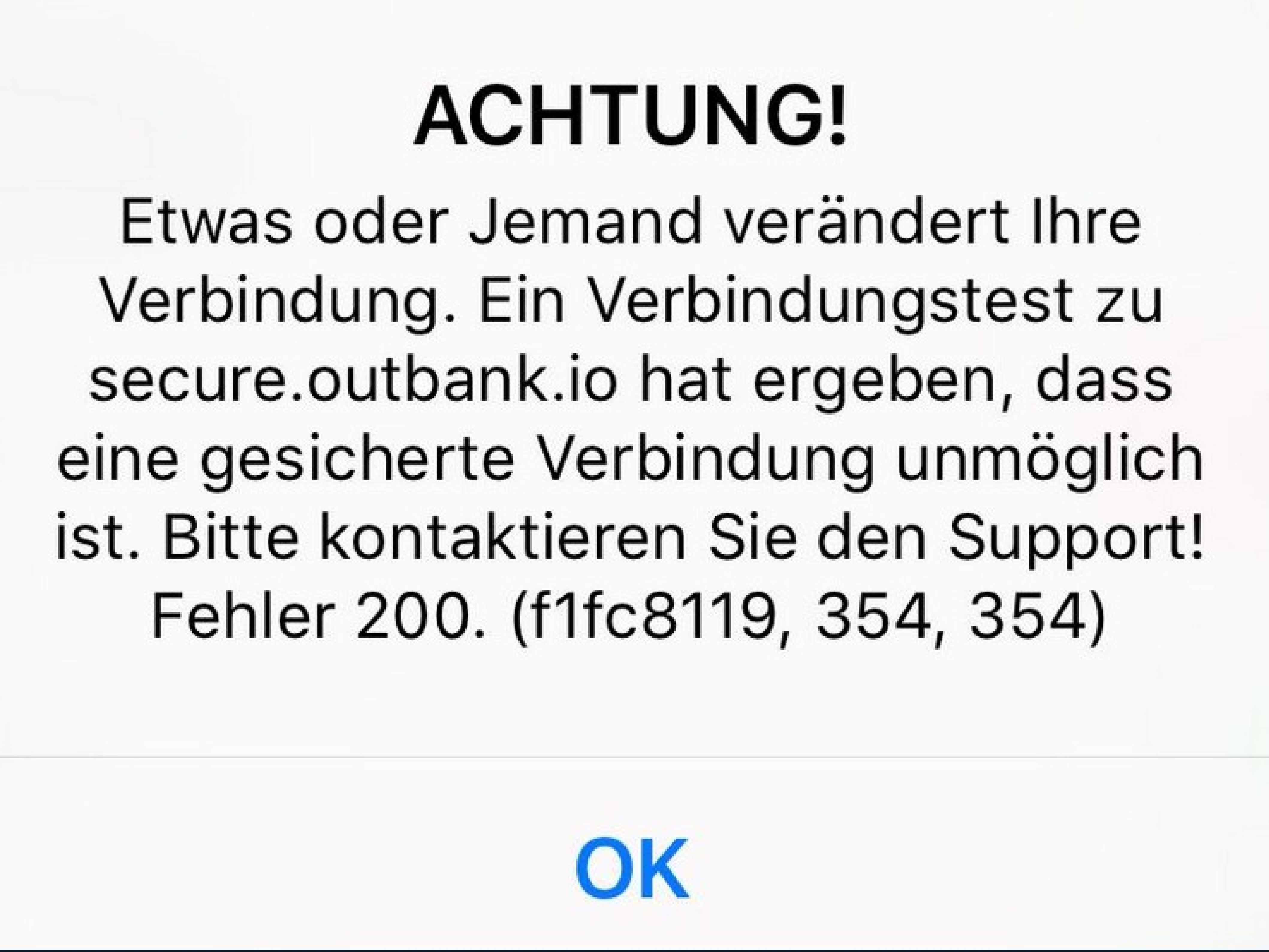
👍 58 👎 83 😄 15 🎉 9 😕 11

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

Category

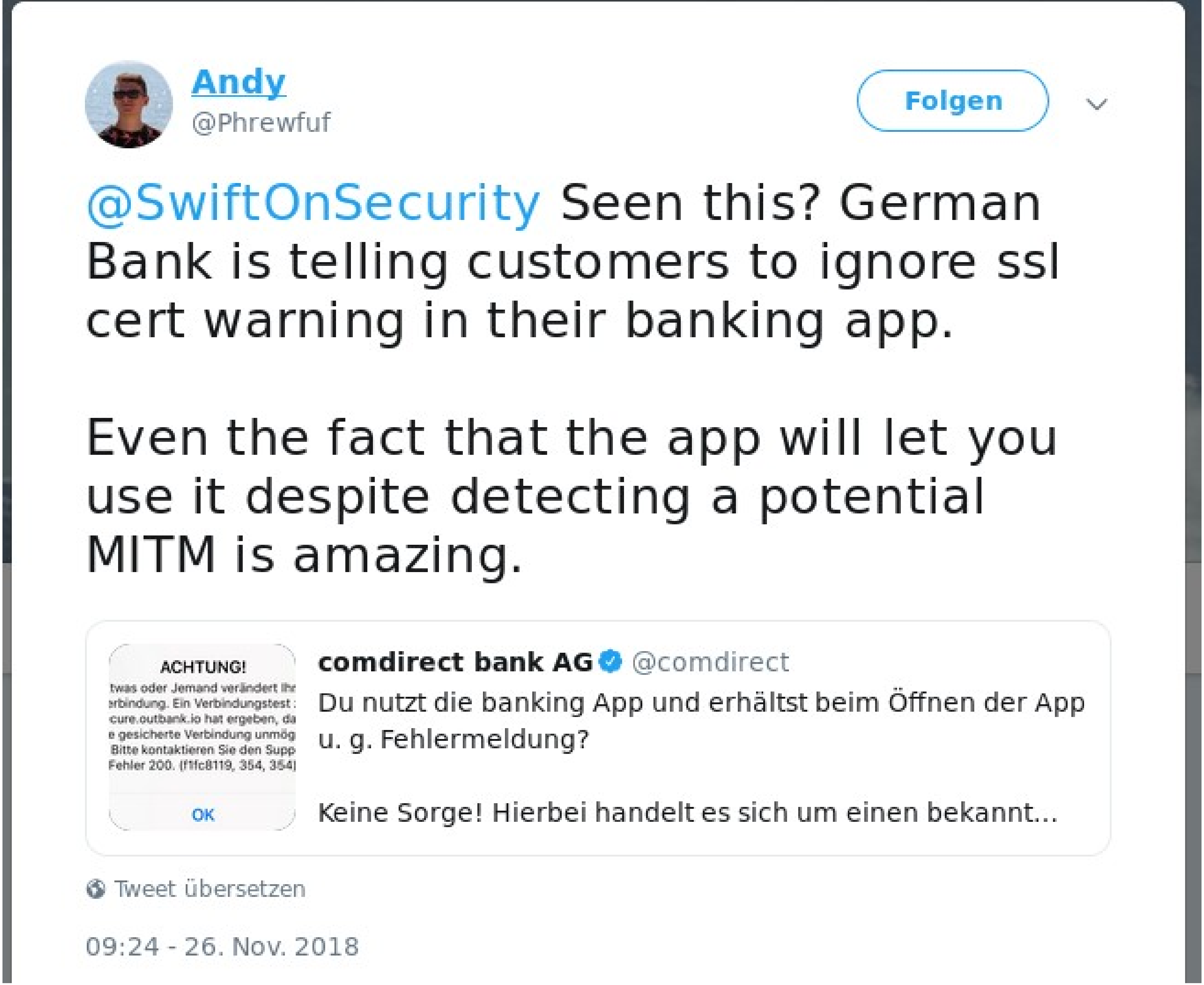
Can I haz
new Bank plz?!1





ACHTUNG!

Etwas oder Jemand verändert Ihre Verbindung. Ein Verbindungstest zu secure.outbank.io hat ergeben, dass eine gesicherte Verbindung unmöglich ist. Bitte kontaktieren Sie den Support! Fehler 200. (f1fc8119, 354, 354)



Andy
@Phrewfuf

@SwiftOnSecurity Seen this? German Bank is telling customers to ignore ssl cert warning in their banking app.

Even the fact that the app will let you use it despite detecting a potential MITM is amazing.

ACHTUNG!
twas oder Jemand verändert Ihr
erbindung. Ein Verbindungstest :
cure.outbank.io hat ergeben, da
e gesicherte Verbindung unmög
Bitte kontaktieren Sie den Supp
Fehler 200. (f1fc8119, 354, 354)

OK

comdirect bank AG @comdirect
Du nutzt die banking App und erhältst beim Öffnen der App u. g. Fehlermeldung?

Keine Sorge! Hierbei handelt es sich um einen bekannt...

09:24 - 26. Nov. 2018

Backdoor

Built in Method to bypass authentification || encryption of a system

Cisco Backdoors

has long Backdoor history

Positive: Intern Auditing !

very creative in finding synonyms

Cisco Backdoors

Examples:

"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

- Easy root access in 3 steps

1) request to /goform/telnet → starts telnet
2) choose freely from 3 existing default accounts on device that are root accounts
Password? Guess!
1234
3) login → profit

- CVE-2018-5770

THE NINETIES CALLED
THEY WANT THEIR PASSWORDS BACK
imgflip.com

Auth Bypass

Authentification Bypass

FIGHT CLUB

Blast from the past!

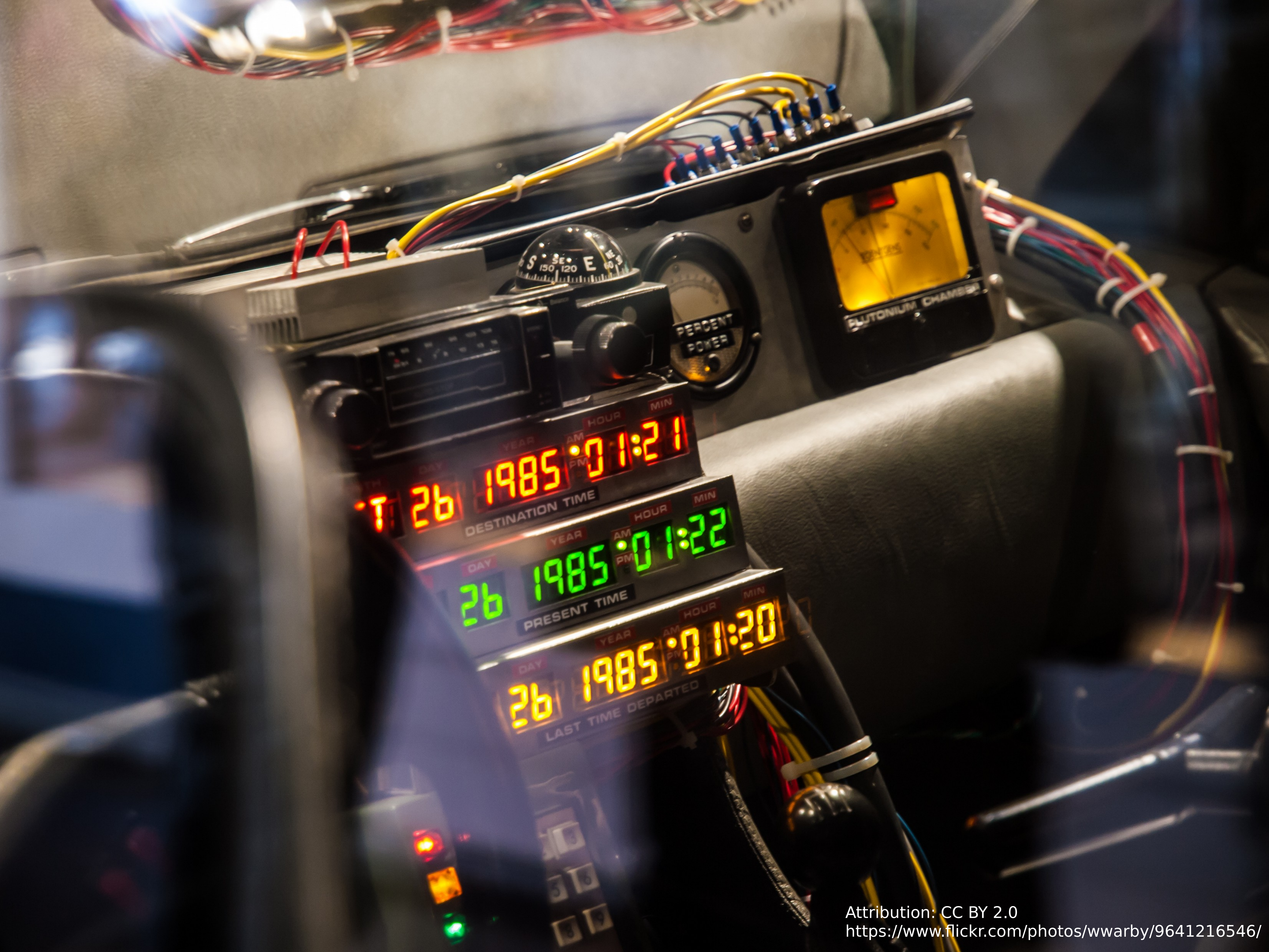
Netscape gained privileges

Netscape Enterprise Server & Netscape FastTrack Server

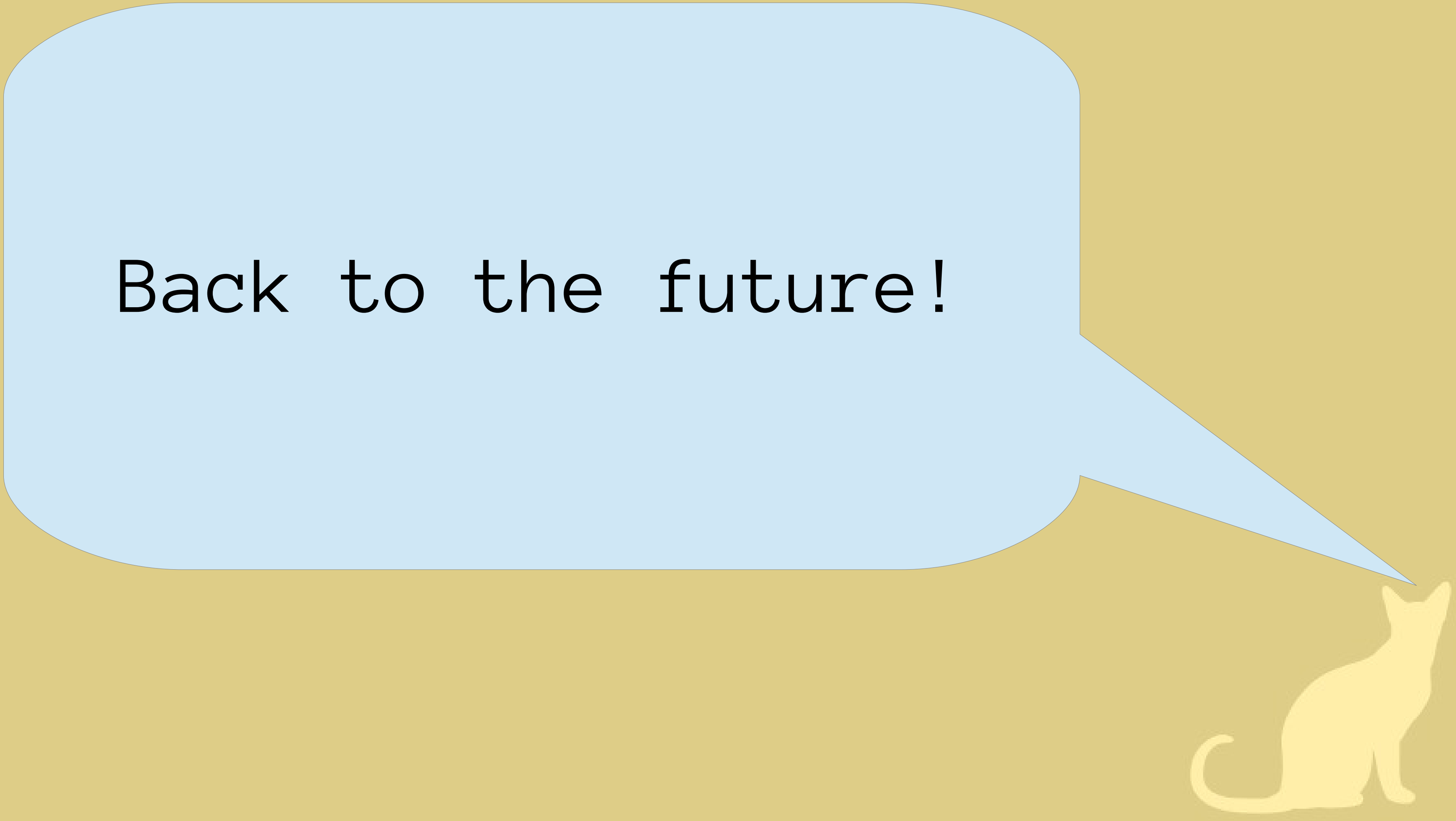
Remote attack

Privileges gained via HTTP Basic Auth

CVE-1999-0853



Attribution: CC BY 2.0
https://www.flickr.com/photos/wwarby/9641216546/


Back to the future!

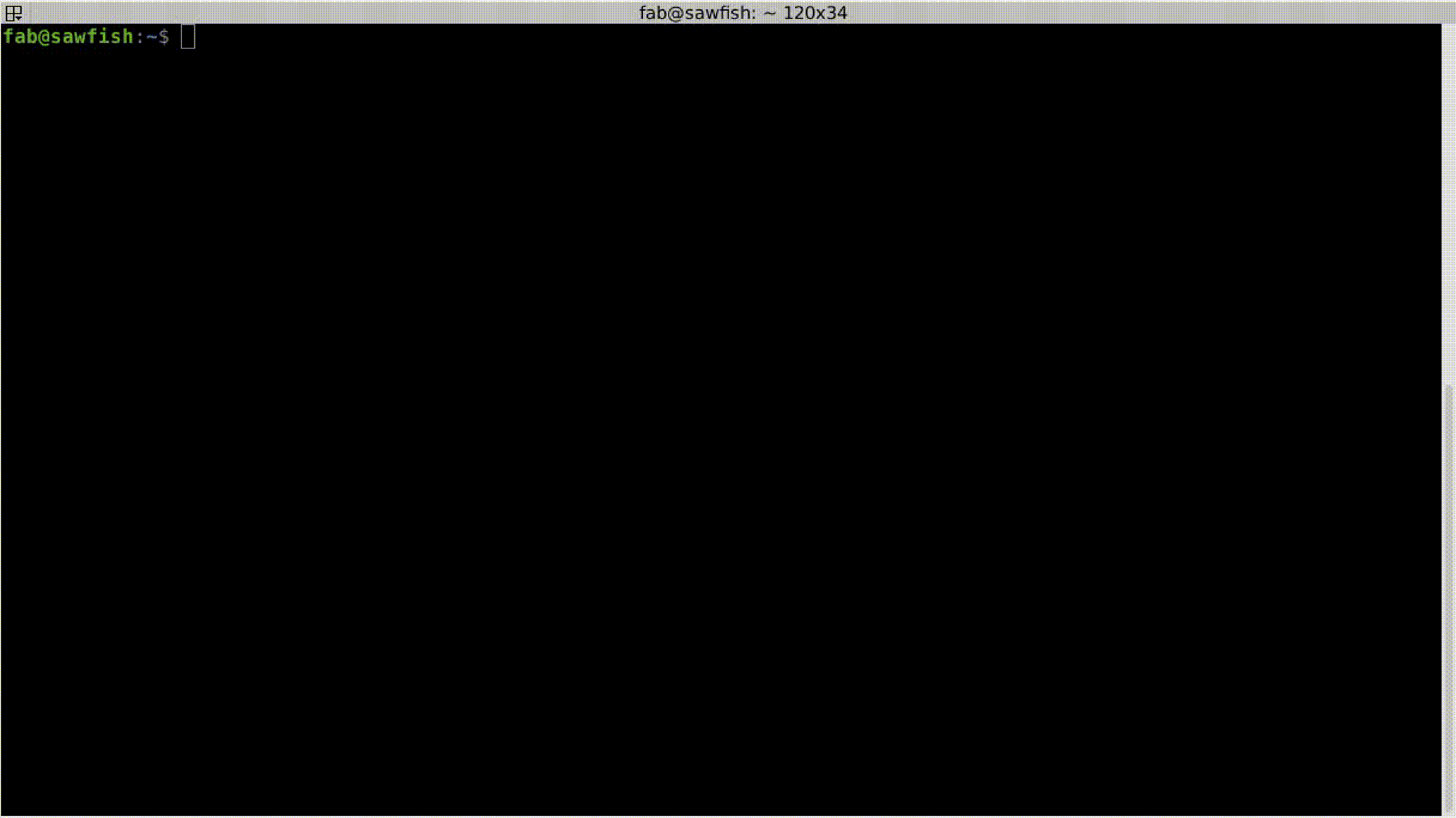
HPE iLO4 Auth Bypass + RCE

remote management console for server

Authentification bypass+RCE

from 2017, broad public knowledge in 2018
- CVE-2017-12542

HPE iLO4 Auth Bypass



```
fab@sawfish:~$
```

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

1999 = 2018

BUFFER
OVERFLOW

Data richness

!data minimisation

digital gold

unnecessary

Google Plus Dataleak

- approx. 500.000 users affected
- partially sensible data stolen
- Google Plus was shutdown

Facebook Dataleak

💰 approx. ~~50.000.000~~ 30.000.000 users affected

💰 60x as much users as G+ Leak affected

💰 They still didn't shut down

DoS

Denial of Service

Netwave IP Camera - DoS

Sending POST request with a huge body size to / URI → Crash camera

PoC on Github

https://github.com/dreadlocked/netwave-dosvulnerability

CVE–2018–6479

RCE

Remote Code Execution

Execute on a remote target own code/programs

Steam RCE

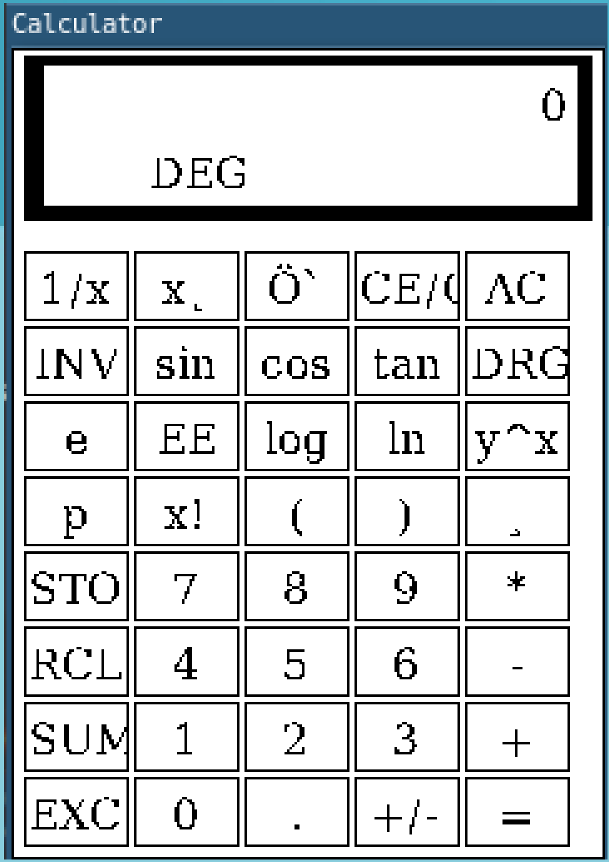
existed 10 years in client

malformed UDP packet enought to trigger exploit

extensive writeup under 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

Overseen, when patched 2 years ago

Trigger: Parsing of Postscript

Found by Tavis Ormadi
Discussion on ML:
https://seclists.org/oss-sec/2018/q3/157

Multiple CVEs assigned

Exploit chain!

Thanks Lena for the Meme :-)

WTF
JUST HAPPENED
imgflip.com

Exploitchain Recap

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

↓

Ghostscript RCE

↓

Virtualbox Escape to host system

↓

Root on host via DirtyCow

Setup

host system: Ubuntu 16.04.4 – unpatched

VirtualBox 5.2.6.r120293

guest system: Debian 9 with GUI – somewhat patched

guest user has sudo with NOPW option

Selfwritten Exploitchain

- Python
- Bash
- (modified) available PoCs

VirtualBox VM Escape

VRAM used for Exploit

Shared Video Buffer (Host+Guest)

Excellent writeup by PoC author:
https://www.voidsecurity.in/2018/08/from-compiler-optimization-to-code.html

CVE-2018-2844

DirtyCow?

Homework for the audience

Hint: `CVE-2016-5195`

Hardware Security

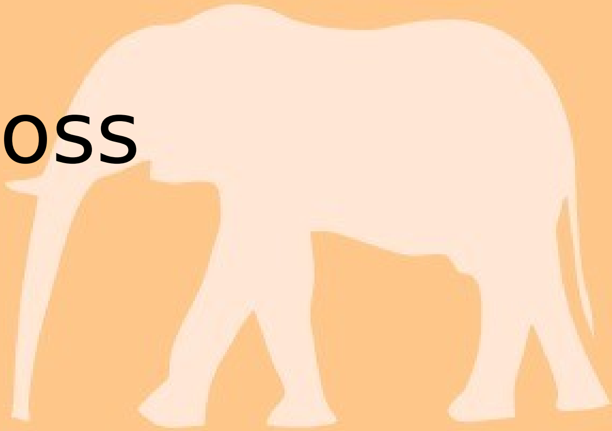
Meltdown && Spectre

Leads to extraction of sensible data

Design fault in modern CPU architecture

Hardware "bug" - speculative execution

Software fixes → performance loss



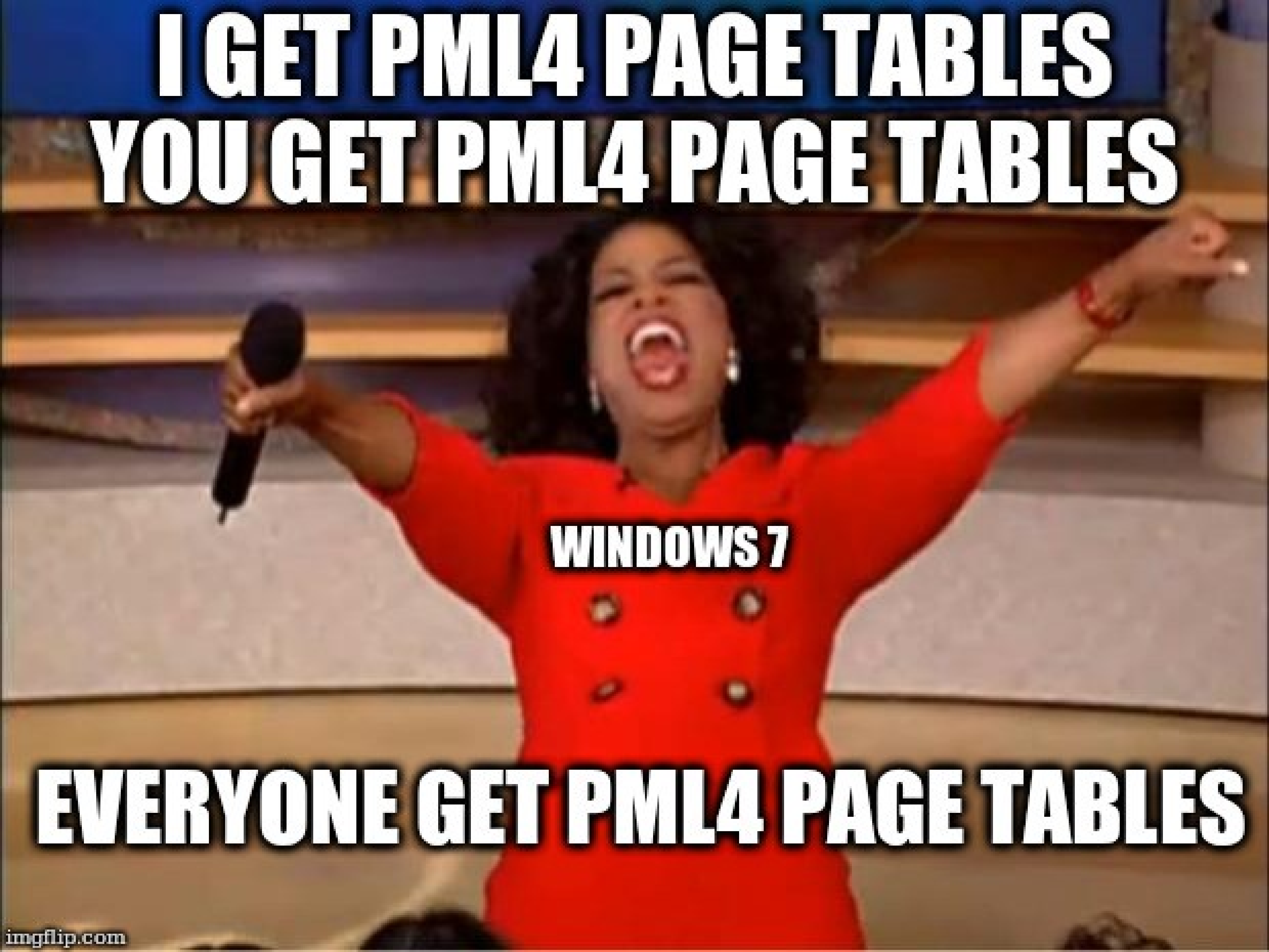
Meltdown "Patch"

Patch for Win 7 & Win Server 2008 R2

PLM4 Page Table accessible for everyone

Everyone could just write in there

LOL


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

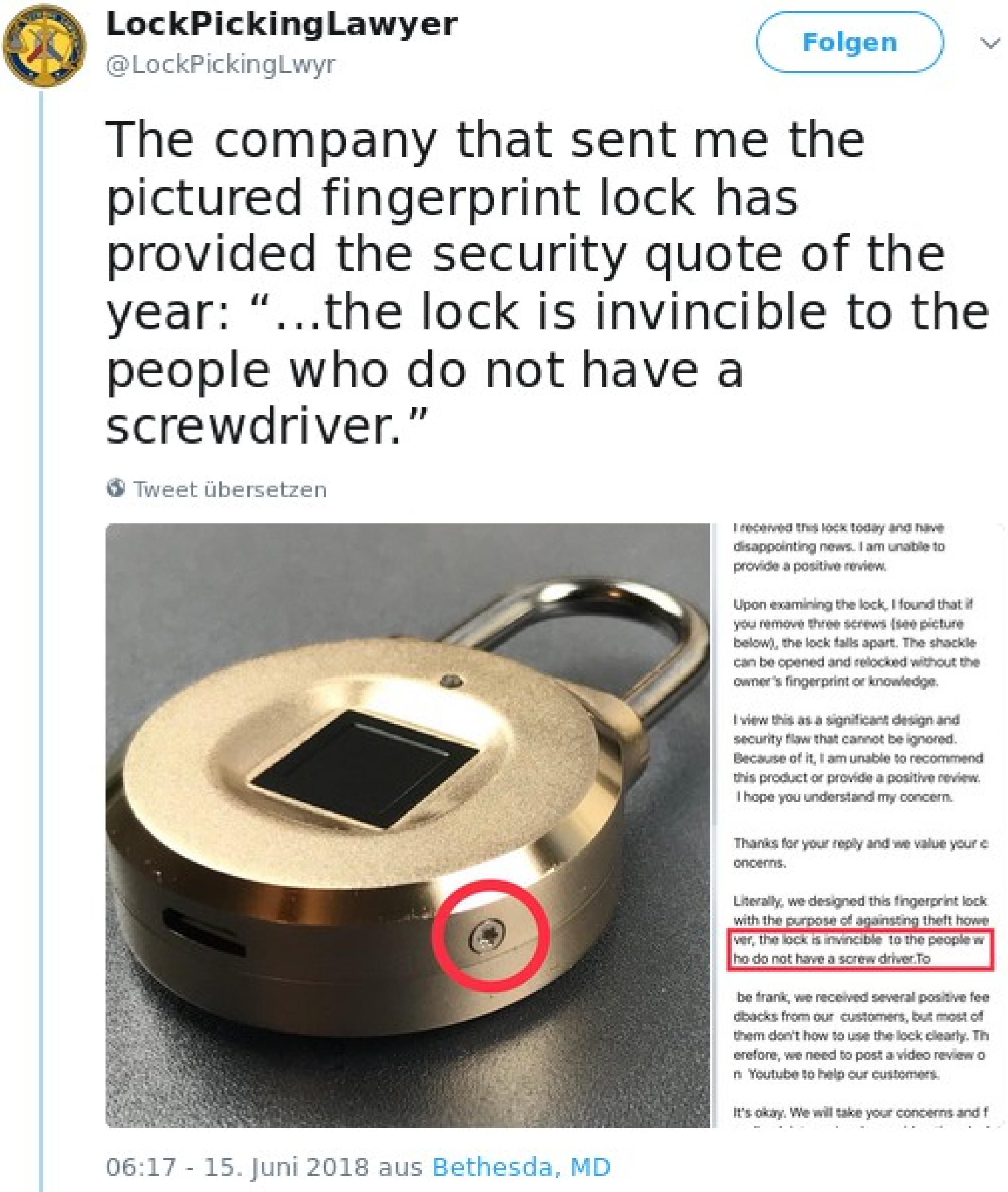
BMW - Telematics Control Unit

BMW vehicles (2012 to 2018)

remote attack

execution (CAN bus) of
arbitrary, unauthorized diagnostic requests

CVE-2018-9318



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."

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

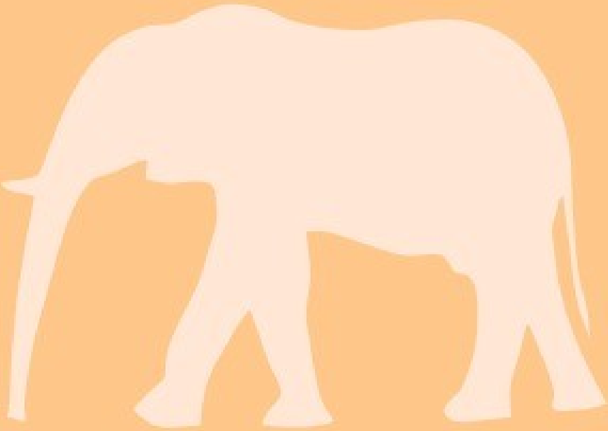
Combine!

Mining Rigs

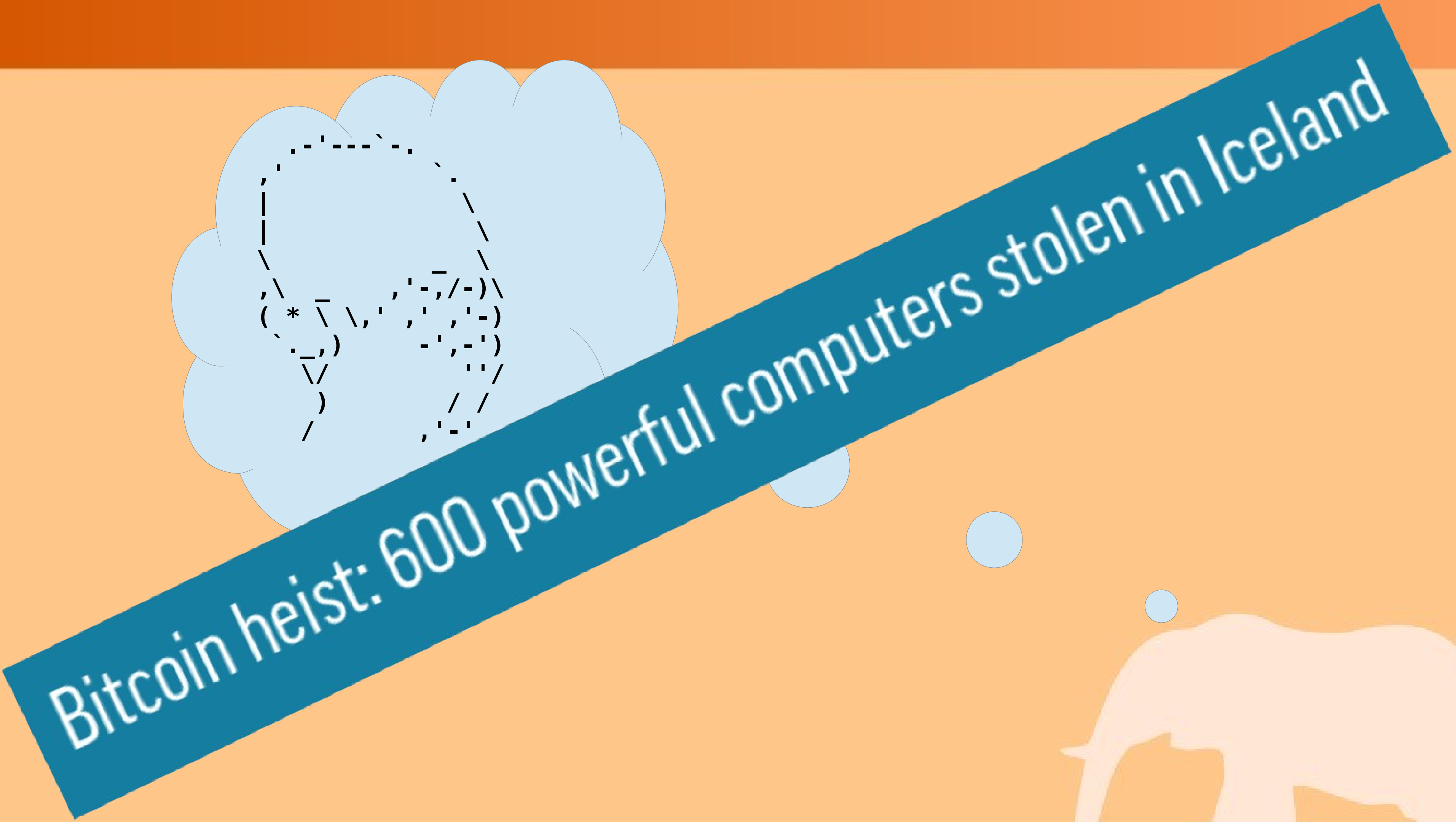
Datacenter

600

Iceland



Stolen Mining Rigs



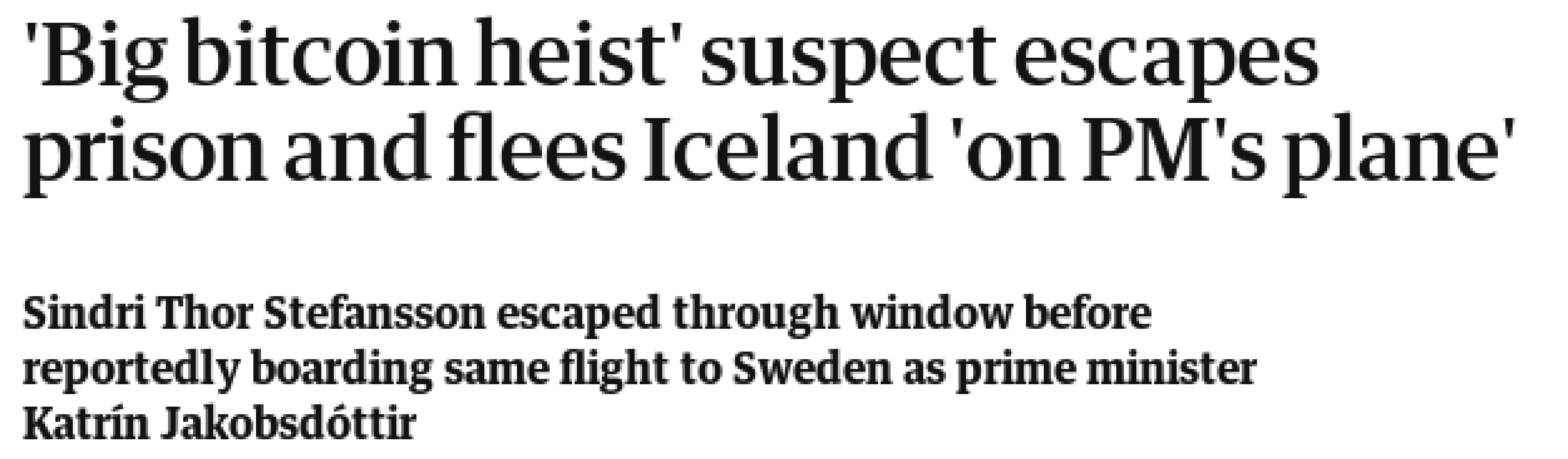
```
  .-'---`-.
 '          `
,             .
|              \
|               \
\           _   \
,\  _    ,'-,/-)\
( * \ \,' ,' ,'-)
 `._,)     -',-')
   \/         ''/
    )        / /
   /       ,'-'
```

Bitcoin heist: 600 powerful computers stolen in Iceland

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

Stolen Mining Rigs

Stolen 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

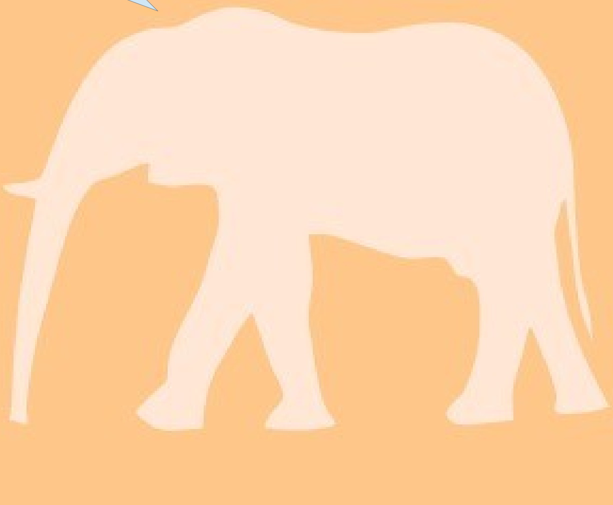
Sound + HDDs = ☠

- Gas-based fire suppression system
- Destroyed HDDs
- Not enough Servers in Sweden
- NASDAQ not operational

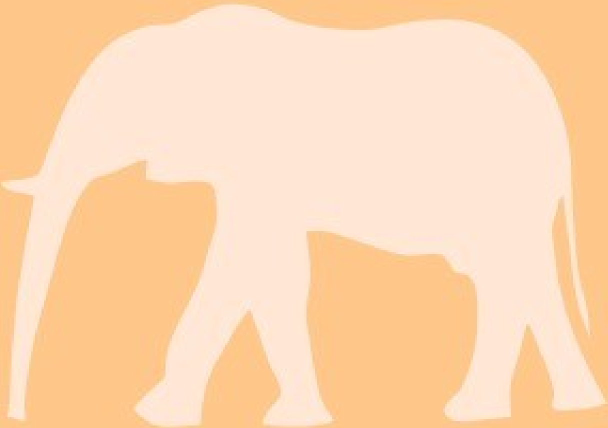
Shouting in the Datacenter: https://www.youtube.com/watch?v=tDacjrSCeq4
Source:
https://www.bleepingcomputer.com/news/technology/loud-sound-from-fire-alarm-system-shuts-down-nasdaqs-scandinavian-data-center/

future pred1cti0n

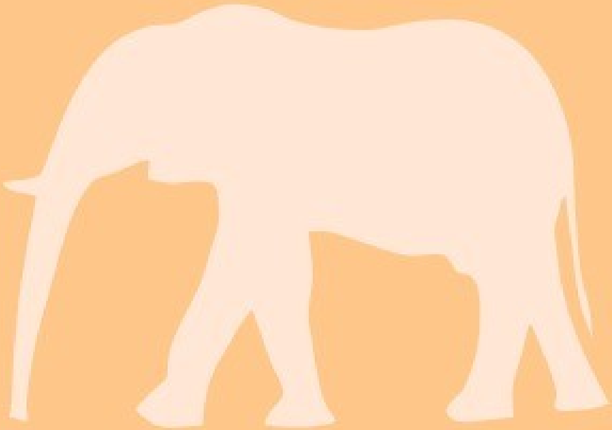
Why should I care?



Security problems affect us all in some way!



Make the world a safer place!



Get some Popcorn and take your time!

Got curious about all this Security foo?
Reading CVEs is fun and interesting!

Where to get the CVE Info?

https://www.cvedetails.com/

QUESTIONS?

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

THANK YOU!

STAY SAFE AND PATCH YOUR SYSTEMS!

CAN I HAZ CONTACT?

Matrix: @hetti:matrix.org

Mastodon: @hetti@chaos.social

Github: https://github.com/hettipeti

Twitter: @Th3peko

Email: more35c3@cyber.coffee ☕

Attribution: Twitter Emoji by Twitter on Github under CC-BY 4.0