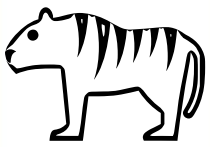
Camp++ 0x72e
24.08.2018

Security Safari in b0rkenLand

Hetti



🚫 Disclaimer 🚫

This talk is (still) **not** about the Safari Browser

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

RCE

Remote Code Execution

Execute on a remote target own code/programs

Command Injection

Inject own controlled commands into system

Auth Bypass

Authentification Bypass

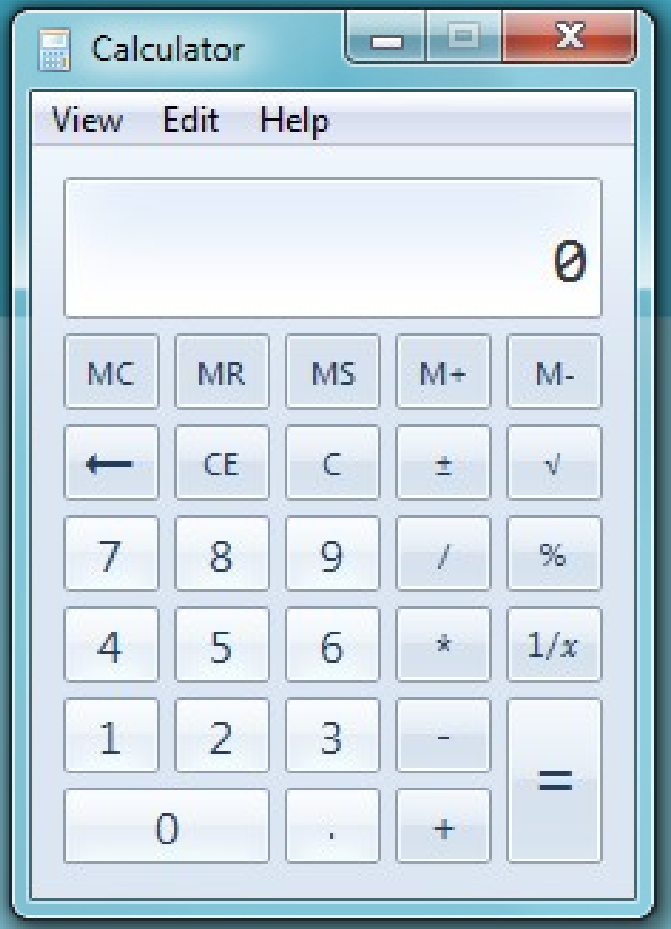
For Example:
Login without credentials
or only with username

DoS

Denial of Service

PoC

Proof of Concept



Screenshot: https://en.wikipedia.org/wiki/Windows_Calculator#/media/File:Windows_7_Calculator.png

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

Meltdown && Spectre

- Leads to extraction of sensible data
- Design fault in modern CPU architecture
- Hardware "bug" - speculative execution
- Software fixes → performance loss


THIS STUFF EATS ALL MY RAM
NOW THEY FOUND A RCE IN IT
imgflip.com

Electron RCE

- Framework for cross plattform apps
- A lot of Software based on Electron
  -Signal, Wire, Slack etc...
- re-enable nodeIntegration via XSS

→ allowed execution of system commands.

- CVE-2018-1000136

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

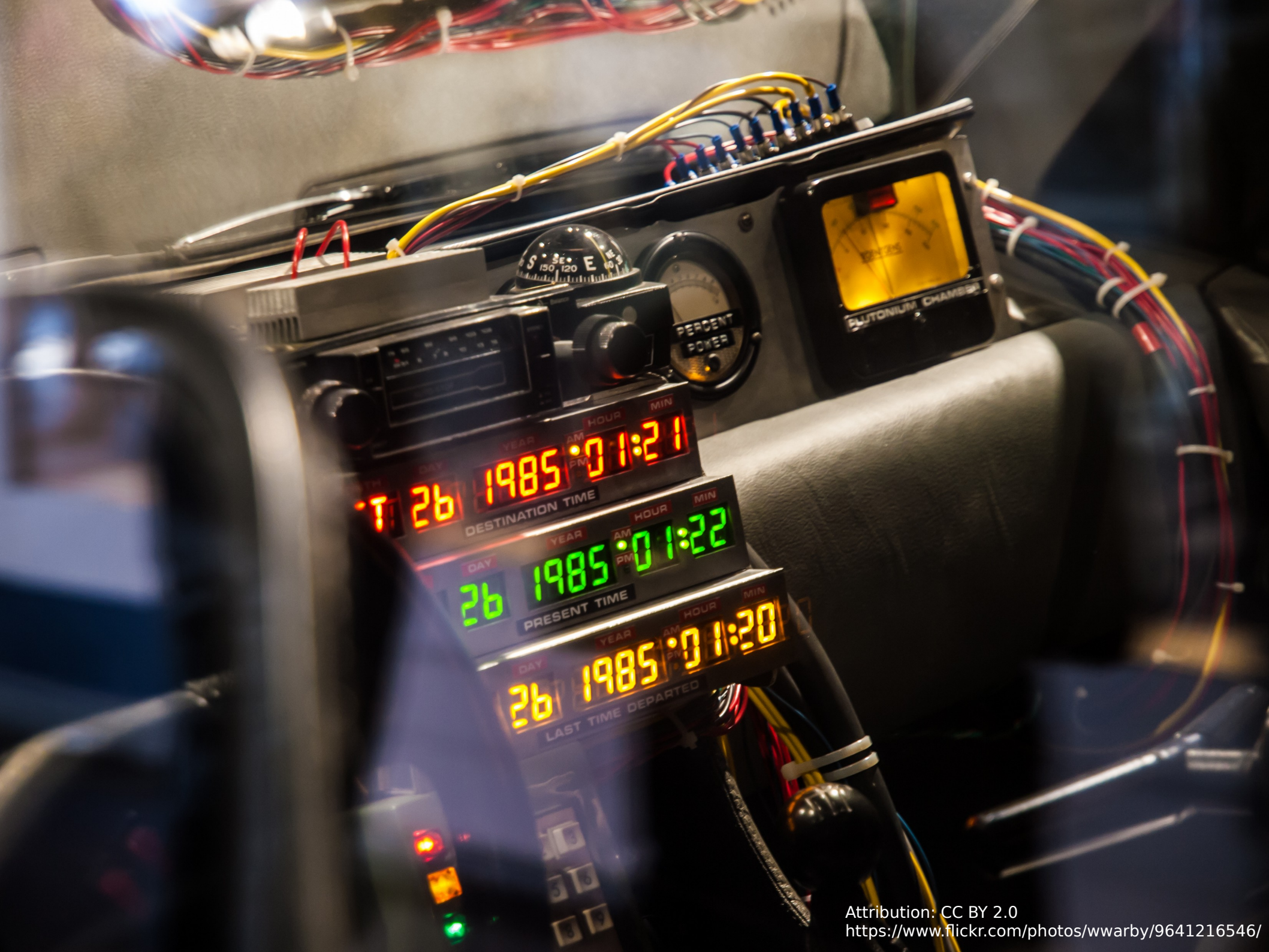
Seagate Personal Cloud Command Injection

- Mediaserver for home use
- no auth required: GET parameters passed unvalidated/unsanitized to Python modules
- led to command injection → running system commands as root.
- CVE-2018-5347

Blast from the past!

Netscape gained privileges

- Netscape Enterprise Server & Netscape FastTrack Server
- Remote attack
- Privileges gained via HTTP Basic Auth
- CVE-1999-0853



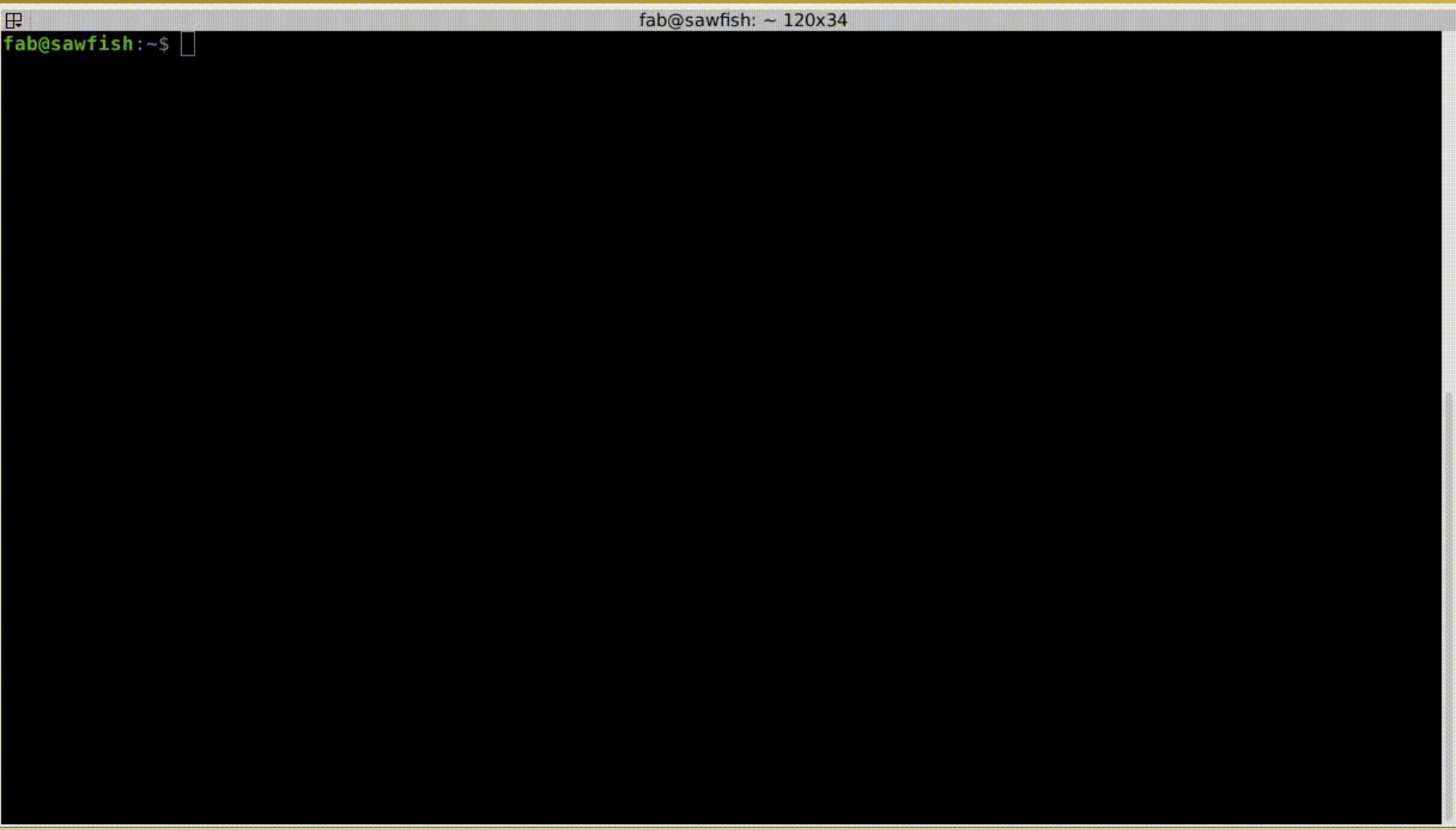
Back to the future!

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



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

1999 = 2018

BUFFER OVERFLOW

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

Hardware Security

BMW - Telematics Control Unit

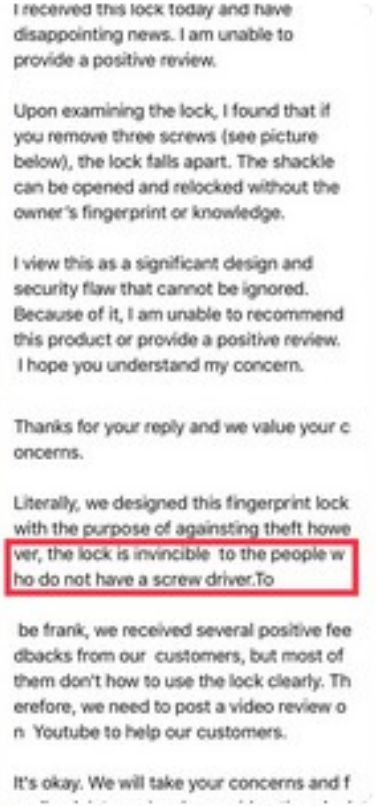
- BMW vehicles (2012 to 2018)
- remote attack
- execution (CAN bus) of arbitrary, unauthorized diagnostic requests
- CVE-2018-9318

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

Combine!

Mining Rigs

Datacenter

600

Iceland

Stolen Mining Rigs

Bitcoin heist: 600 powerful computers stolen in Iceland

REYKJAVIK, Iceland (AP) — Some 600 computers used to "mine" bitcoin and other virtual currencies have been stolen from data centers in Iceland in what police say is the biggest series of thefts ever in the North Atlantic island nation.

Some 11 people were arrested, including a security guard, in what Icelandic media have dubbed the "Big Bitcoin Heist." A judge at the Reykjanes District Court on Friday ordered two people to remain in custody.

The powerful computers, which have not yet been found, are worth almost $2 million. But if the stolen equipment is used for its original purpose — to create new bitcoins — the thieves could turn a massive profit in an untraceable currency without ever selling the items.

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

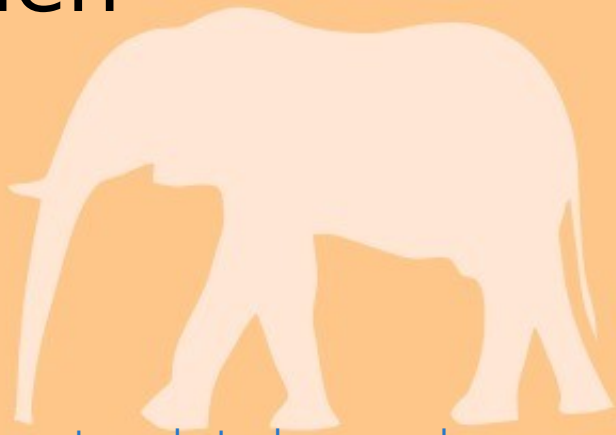
The suspected mastermind behind the theft of 600 computers used to mine bitcoin in Iceland has escaped from prison and fled to Sweden on an aeroplane reportedly carrying the Icelandic prime minister.

Sindri Thor Stefansson escaped through a window of the low-security Sogn prison in rural southern Iceland before boarding a flight to Sweden at the international airport in Keflavik located 59 miles from the prison on Tuesday. Police said he travelled under a passport in someone else's name, but was identified via surveillance video.

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/

Why should I care?

Security problems affect us all in some way!

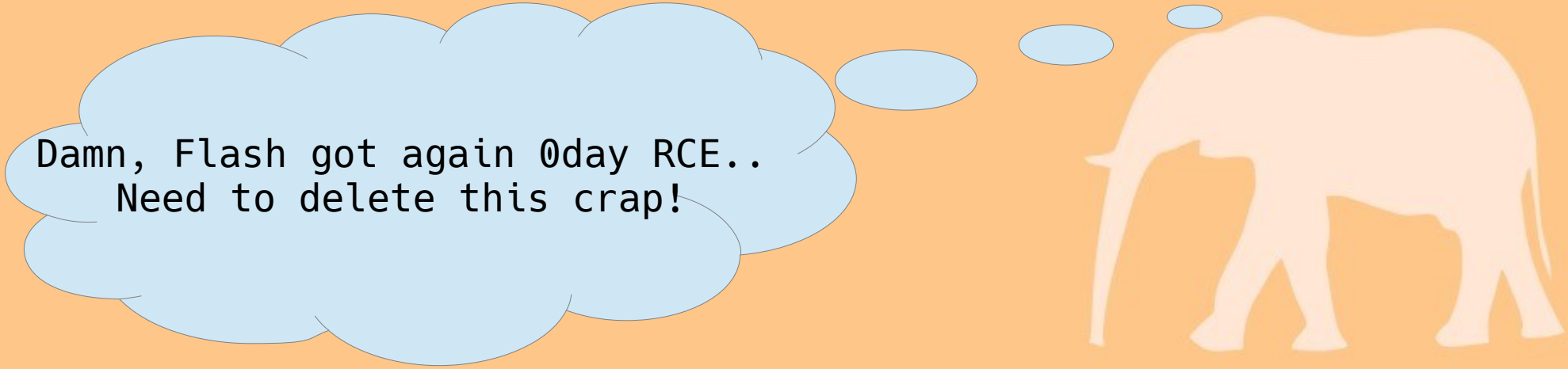
Make the world a safer place!

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?

THANK YOU!

STAY SAFE AND PATCH YOUR SYSTEMS!

CAN I HAE CONTACT?

Matrix: @hetti:matrix.org

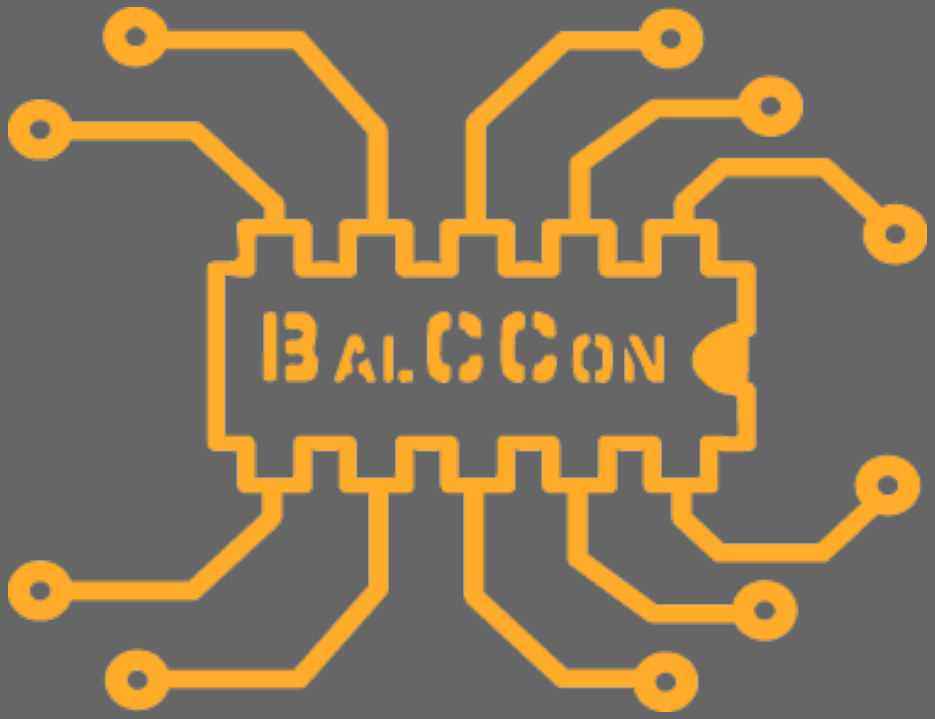
Mastodon: @hetti@chaos.social

Twitter: @Th3peko

Email: camppp18@cyber.coffee

BalCCon 2k18

Find yourself



14-16 September

Novi Sad – Serbia

Come and bring your friends!