


Security Safari in b0rkenLand

Hetti

Security 101

DoS

Command Injection

Auth Bypass

Backdoor

CVE

RCE

CVSS

PoC

CVE

Common Vulnerabilities and Exposures

- Industry standard
- naming convention
- publicly known securit vulns
- Example: CVE-2017-0143

CVSS

Common Vulnerability Scoring System

- free+open industry standard
- Scoring: 0-10
- based on formula depending on different metrics

RCE

Remote Code Execution

Execute on a remote target own code/programs

Command Injection

Inject own controlled commands into System

For examle via some command interface on website

Auth Bypass

Authentification Bypass

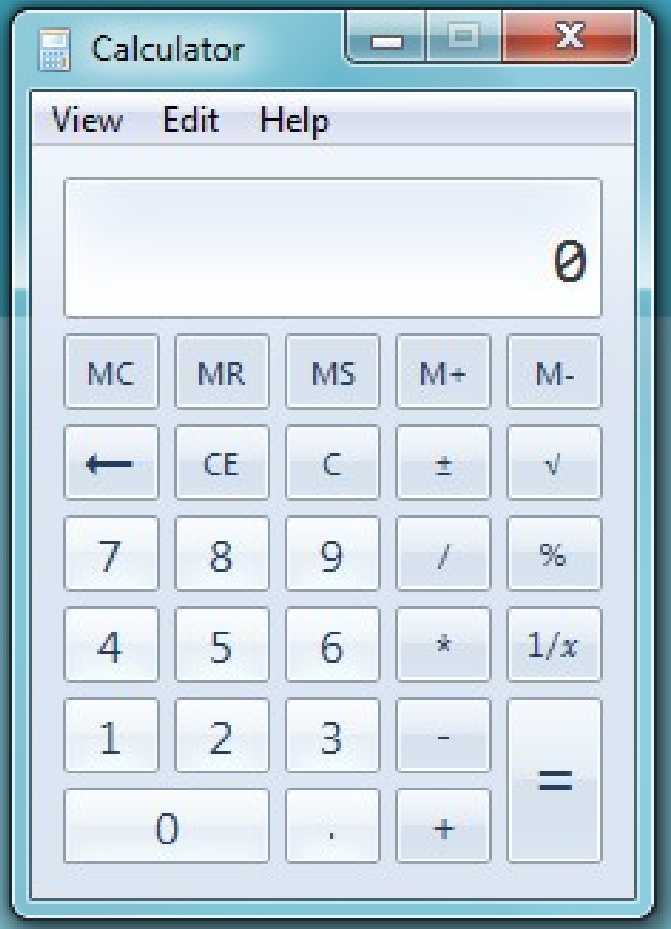
For Example:
Login without credentials
or only with username

DoS

Denial of Service

Make system unavailable temporary/permanently

PoC



Proof of Concept

Normally as Code

Classic PoC for RCE on Windows:

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
- very creative in finding synonyms
- 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

Meltdown && Spectre

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

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
- Patched by Steam team 8h after Report
- 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

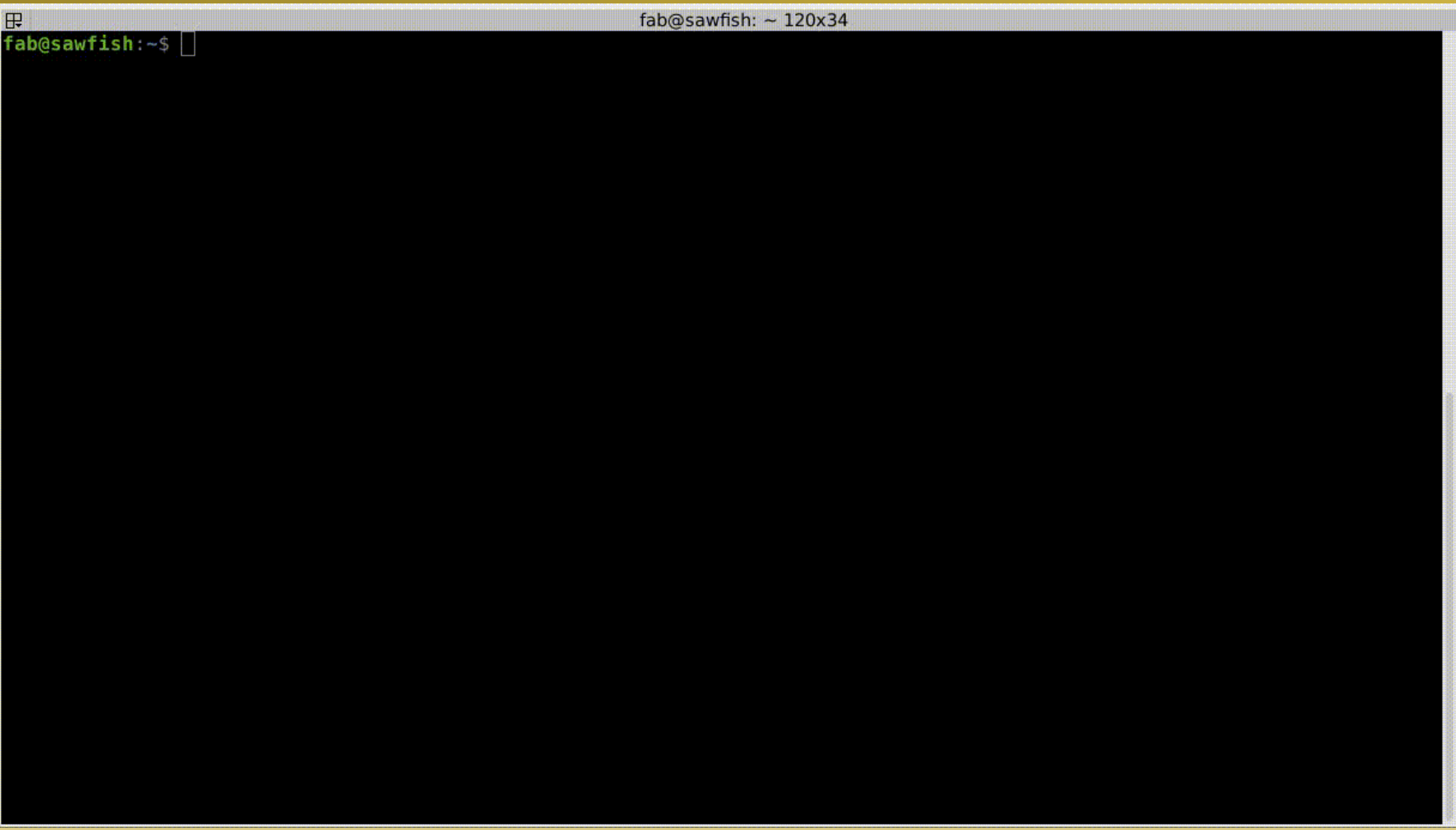
Seagate Personal Cloud Command Injection

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

HPE iLO4 Auth Bypass + RCE

- remote management console for server
- Authentification bypass+RCE
- found by Airbus Research Team
- invested 5 man-months for research
- from 2017, broad public knowledge in 2018 CVE-2017-12542

HPE iLO4 Auth Bypass



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

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

BMW - Telematics Control Unit

- BMW vehicles from 2012 to 2018 affected if present
- remote attack via a cellular network.
- CAN buses with the execution of arbitrary, unauthorized diagnostic requests remotely
- CVE-2018-9318

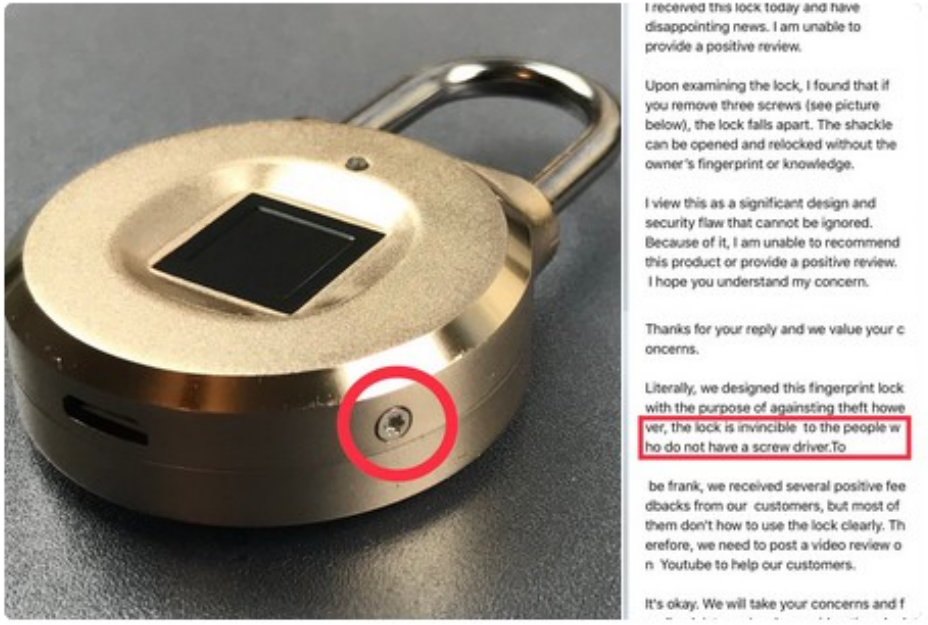
Hardware Security

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

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

Twitter: @Th3peko

Email: fsec18@cyber.coffee