Risk and Vulnerability Management

Sven Gabriel, Nikhef, EGI CSIRT

June 2022

Overview

Introduction

Risk and Vulnerability Management is a wide area. We will only have a generic view on Risk Management and some hints why this would be very helpful for the organisations Operational Security team. As for vulnerability management we will take a look on how its done in EGI.
A much more complete online training on Vulnerability Management is available at GÉANT:
https://learning.geant.org/domain-name-system-dns-protection-operational-network-

Risk, Threats and all the rest

Risks are about things that can possibly go wrong, in our context it is about threats to our infra. Here, A security risk is the loss potential to an organization's asset(s) that will likely occur if a threat is able to exploit a vulnerability.

- STRIDE: A model of what can go wrong:
- Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
- Is used in threat modelling, see Adam Shostack's book Threat Modeling: Designing for Security https://shostack.org or https://www.youtube.com/watch?v=DMFF8zQqEVQ

Incident Response for High impact incident

- To get started, . . . lets look at the debriefing of a successful ransom attack and the problems you may run into, like:
- How to prioritize what systems to bring back first. (Business Continuity Plan)
- What is lost? GDPR relevant data loses need to be reported to the authorities.
- do useable back-ups of **important** (for business continuity) datasets exist?
- Note, at this stage its not about what security controls failed.
- Risk analysis helps to know your assets and protective measures in place.

What is Risk Analysis?

Risk Analysis is a process. An objective analysis of the effectiveness of the current security controls that protect an organization's assets and a determination of the probability of losses to those assets. [1]
When doing it for an organisation, this is rather a project with involvement of senior management and other key-personal.

[1] The Security Risk Assessment Handbook A Complete Guide for Performing Security Risk Assessments, Douglas J. Landoll

Phases/Steps in Risk Analysis

There are multiple methods and frameworks available for Risk Management [2]. Remember, this is a project which requires the usual project management (with senior management contribution/support). The methods differ in details/organisation of the following phases. Which method to use is also subject to the goal of the Risk assessment (Compliance with security regulations, ISO-27K, NIST-800, etc)

[2] https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

Info Gathering Phase

Large parts of the info gathering is already done in the project planning part. Information Gathering, Identify:

- Assets
- Threats [3].
- identify Critical systems (ex. systems that automate critical business functions)

[3] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Get Info on available Controls

- Administrative (policies, procedures)
- Technical (Design, Architecture, Configuration, AuthNZ)
- Physical (physical access control, CCTV etc)

Risk Analysis

Bringing together the gathered data/information.

- Asset valuation, example: Low (little to no impact), Medium, High, Critical (Indicates that compromise of the asset would have grave consequences). Various valuation approaches.
- Threat and Vulnerability mapping,
- Risk Calculation. (Here the above information is used to get a quantitative value)
- Risk Mitigation: Safeguard selection, Safeguard effectiveness(cost-value ratio)

Risk mitigation

- Safeguard/Control selection
- Safeguard/Control effectiveness (cost-value ratio)
- Risk reduction (improve existing controls, apply additional controls)
- Result: Residual security risk (that remains after implementation of recommended safeguards). This will be treated in the next step.

Recommendations, Reporting and Resolution

Senior manager must decide to reduce the security risk, accept the residual security risk, or delegate the security risk to someone else (example: insurance).

- Risk transfer.
- Risk acceptance.
- Risk assignment.

Finally

The Risk assessment report will help the Operational Security team to prioritize the available resources to:

- Security Monitoring (ex. access control)
- System audits, log processing, alerting
- Back-up Strategy

Vulnerabilities and all the rest

Definitions:
ENISA: “The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.”
Iso 27005 (more appropriate in context of the Riskamanagement we just talked about:
ISO/IEC 27005: “A weakness of an asset or group of assets that can be exploited by one or more threats, where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization’s mission.”

Scope: Vulnerability Management in EGI

- We (EGI) are a Linux shop, Microsoft does things differently, will not be discussed here.
- Also Web vulnerabilities are out of scope here, we are mainly concerned about compute clusters and virtualisation vulnerabilities. An interesting aspect is always IAAS deployed in the cloud.
- Interesting edge cases are of course design vulnerabilities (in hardware), vulnerabilities in systems that reached EOL, or vulnerabilities that can not be fixed easily like firmware in Iot devices (with googable default passwords).

Vulnerability Lifecycle

The time from vunerability disclosure to available patch varies from days (software under support) to never (unsupported software, hardware design flaws like spectre, meltdown)
Urgency of actions: Patching an infra can have an impact on the availability. Balance requests to urgent action!

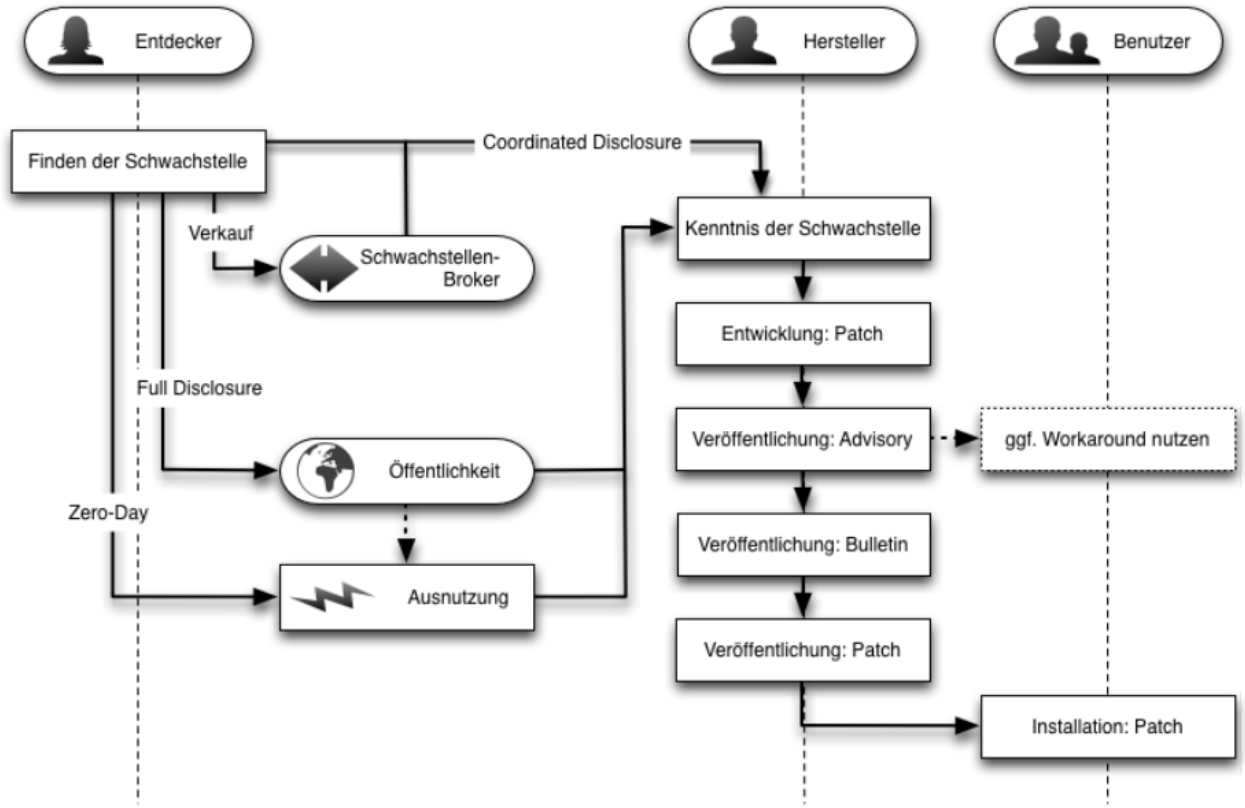
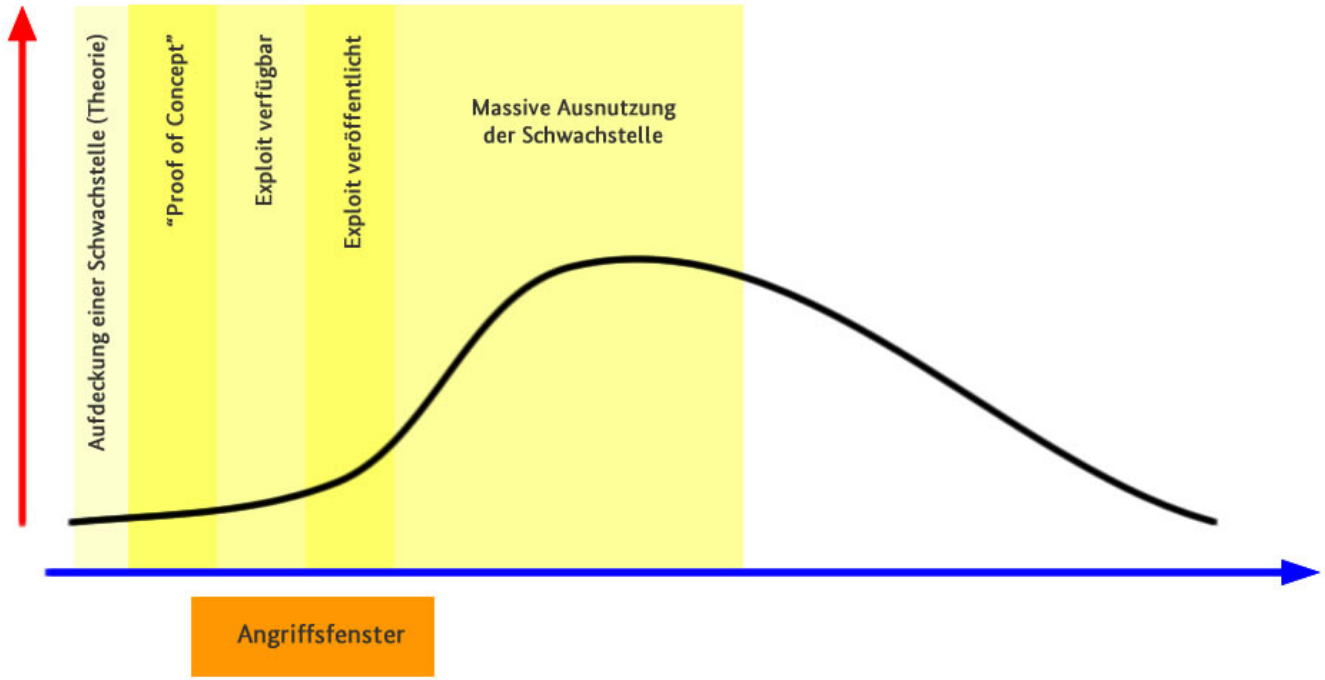


Abbildung 1: Lebenszyklus einer Schwachstelle

Vulnerability, urgency for patching

Urgent action is required for: Vulnerabilities (assessed as critical by EGI) **and** for which an exploid is published.

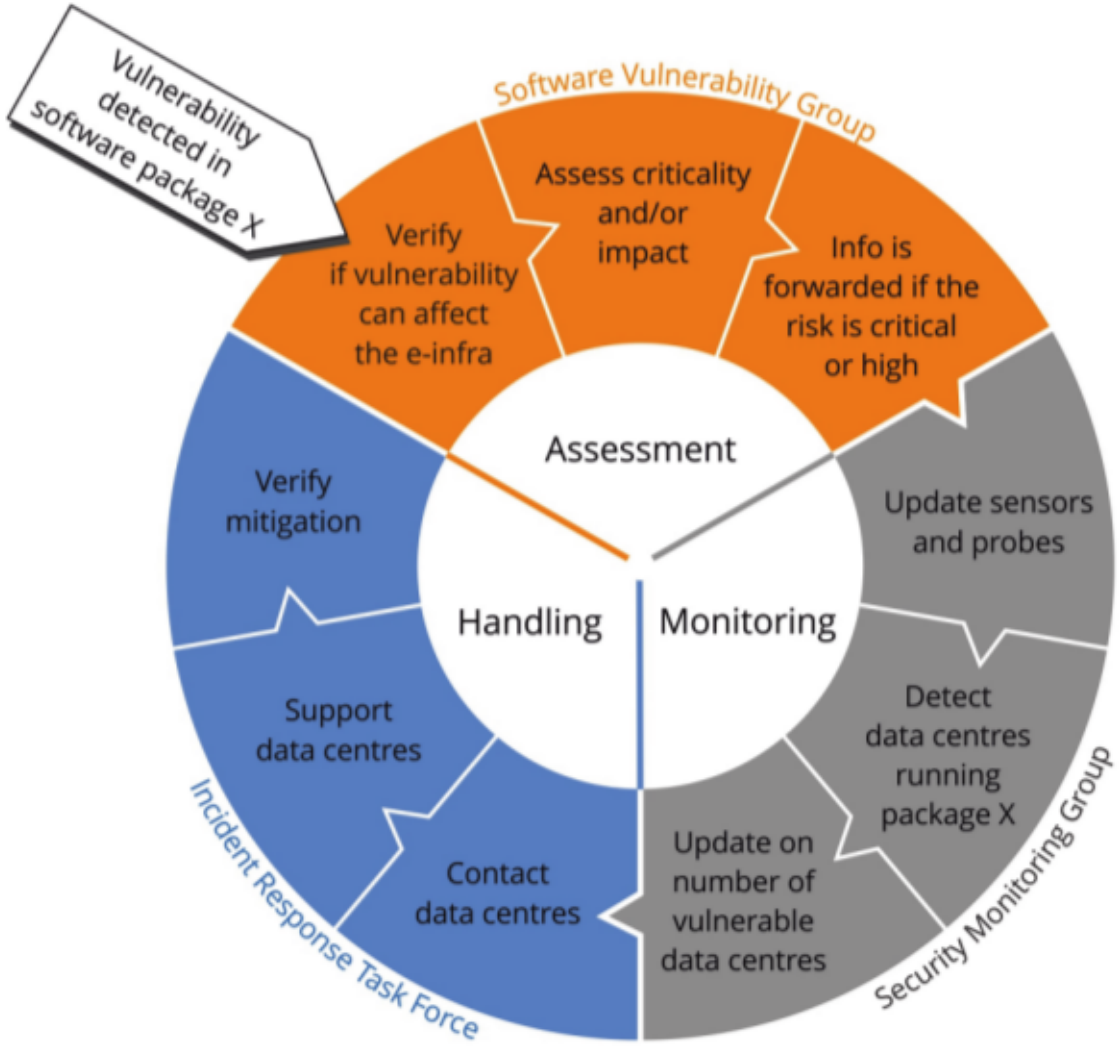


5

[5] https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Buerger-CERT-Abos/Buerger-CERT-Sicherheitshinweise/Risikostufen/risikostufen.html

Vulnerability handling, continuous process

https://csirt.egi.eu/activities/:



Vulnerability handling, Terminology

- Vulnerabilities have an identifier: CVE-YYYY-NNNN (Common Vulnerabilities and Exposures), a list. [6]
- Criticality is often expressed as a numerical value resulting from the assessment using CVSS [7]
- Other Specifications, Tools: CPE (Common Platform Enumeration), CWE (Common Weakness Enumeration), dictionary.)
- machine readable (xml), format: cpe:/ hardware-part [OS-part [/ application-part]]

[6] https://cve.mitre.org/

[7] https://www.first.org/cvss/

Vulnerability handling, Advisories

Advisories have a certain format, Depending on your role, the advisories can be:

- informal: this is the problem, here is how you can fix it.
- require action: this is the problem, fix it now, or ...

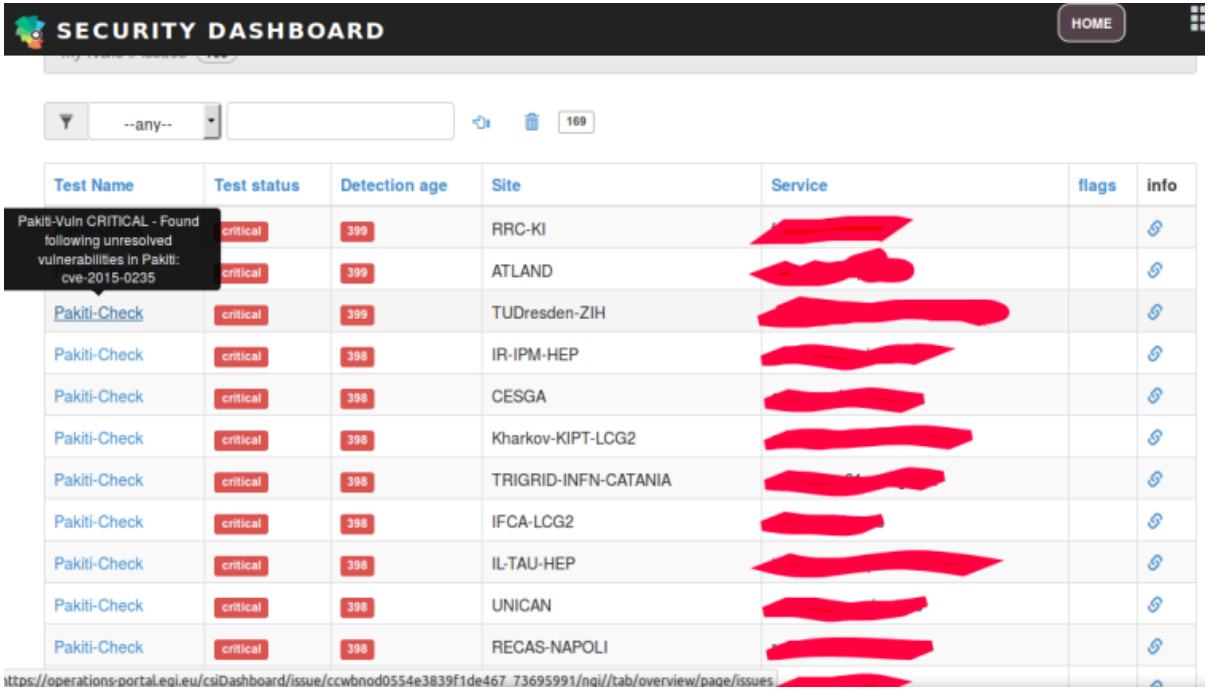
Vulnerability handling, Policies

If you want to require (mitigation or resolution action) from the recipients of your advisory within a certain time, . . . you need to be backed up by managment.

- Management Board approved procedure
- Secure operation policies

Vulnerability handling in action

Patch Status monitoring: Local root exploit:



Vulnerability handling in progress

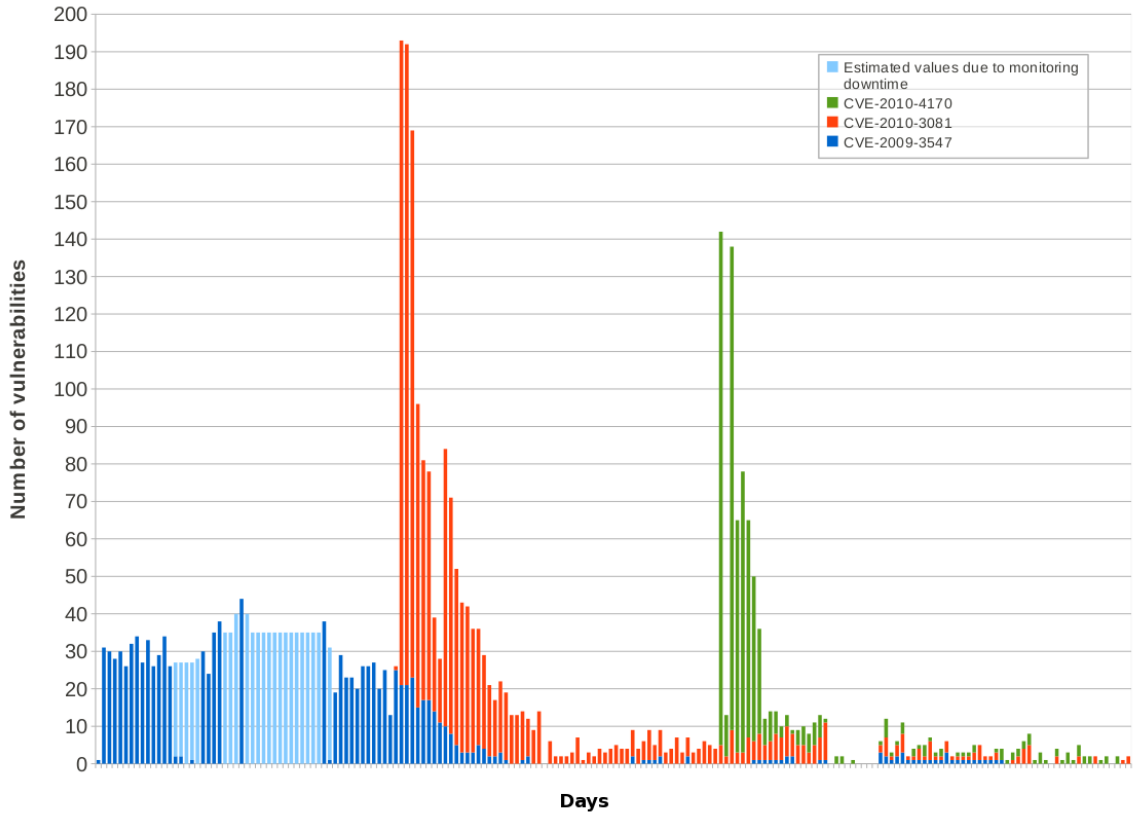
- Advisories send to Resource Centres
  https://wiki.egi.eu/wiki/SVG:Advisories
- Situation monitored in SecMon
- After n days, no sites expose problematic software versions.

OK, the infra is clean, we are done with it.

Aren't we?

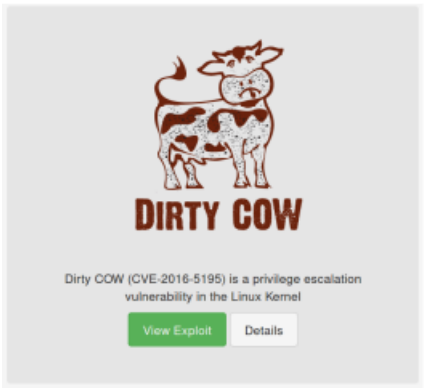
Vulnerability handling in action

Hm, not really . . . .

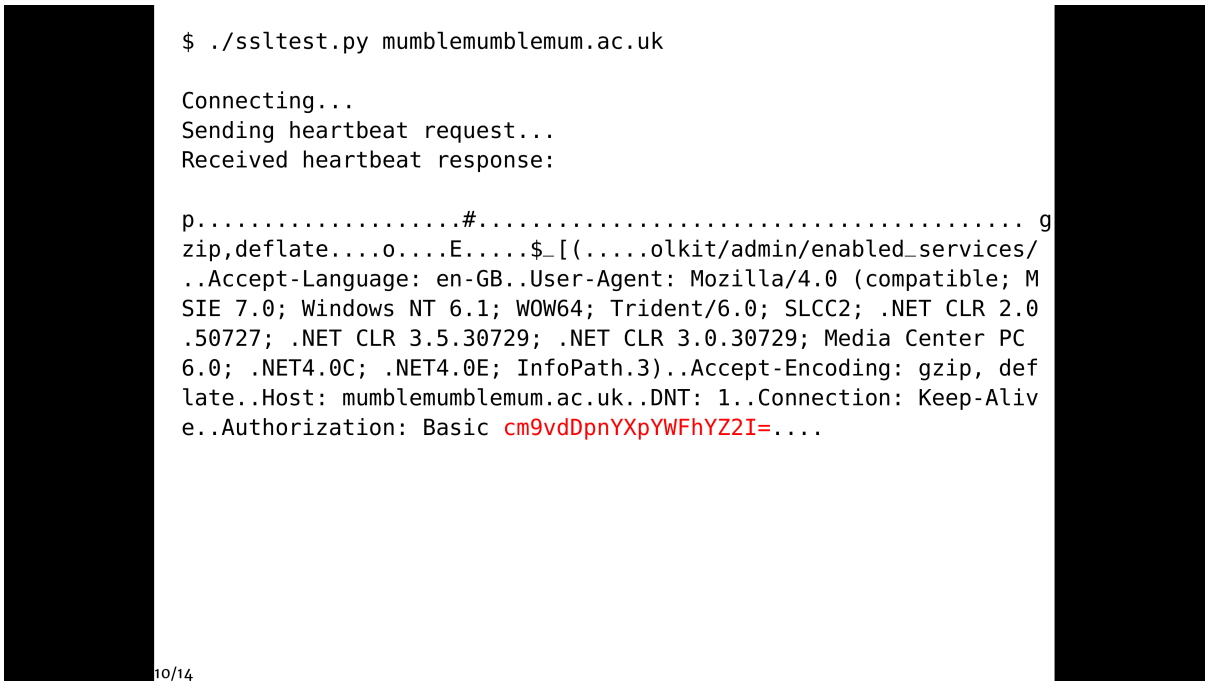


Vulnerabilities with Icons I

Interesting vulnerabilities got names . . . and icons.



Vulnerabilities with Icons II

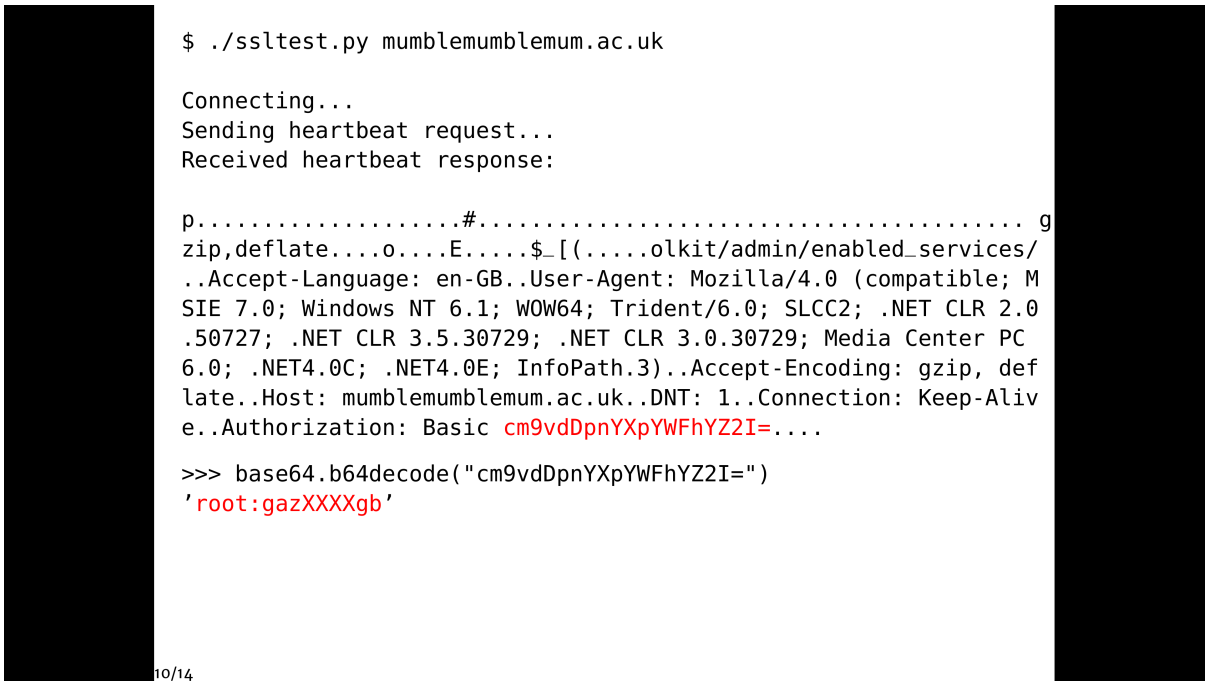


```
$ ./ssltest.py mumblemumblemum.ac.uk

Connecting...
Sending heartbeat request...
Received heartbeat response:

p..................#..................................... g
zip,deflate....o....E.....$_[(.....olkit/admin/enabled_services/
..Accept-Language: en-GB..User-Agent: Mozilla/4.0 (compatible; M
SIE 7.0; Windows NT 6.1; WOW64; Trident/6.0; SLCC2; .NET CLR 2.0
.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C; .NET4.0E; InfoPath.3)..Accept-Encoding: gzip, def
late..Host: mumblemumblemum.ac.uk..DNT: 1..Connection: Keep-Aliv
e..Authorization: Basic cm9vdDpnYXpYWFhYZ2I=....
```

Vulnerabilities with Icons II



```
$ ./ssltest.py mumblemumblemum.ac.uk

Connecting...
Sending heartbeat request...
Received heartbeat response:

p..................#..................................... g
zip,deflate....o....E.....$_[(.....olkit/admin/enabled_services/
..Accept-Language: en-GB..User-Agent: Mozilla/4.0 (compatible; M
SIE 7.0; Windows NT 6.1; WOW64; Trident/6.0; SLCC2; .NET CLR 2.0
.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C; .NET4.0E; InfoPath.3)..Accept-Encoding: gzip, def
late..Host: mumblemumblemum.ac.uk..DNT: 1..Connection: Keep-Aliv
e..Authorization: Basic cm9vdDpnYXpYWFhYZ2I=....

>>> base64.b64decode("cm9vdDpnYXpYWFhYZ2I=")
'root:gazXXXXgb'
```

Design Flaw Vulnerabilities

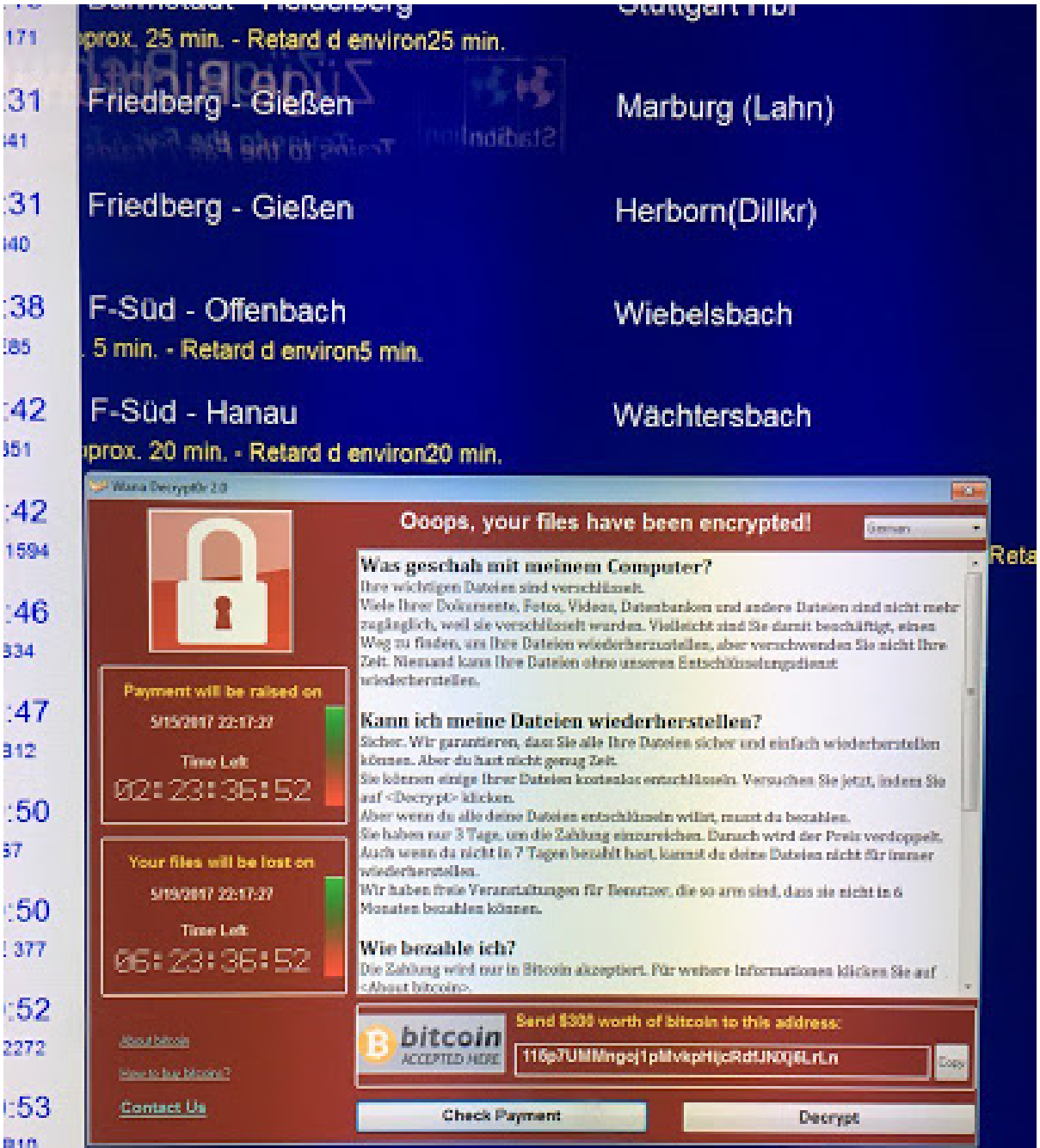
Meltdown and Spectre:

- Solution: “The underlying vulnerability is primarily caused by CPU architecture design choices,” CERT researchers wrote. “Fully removing the vulnerability requires replacing vulnerable CPU hardware.”
- Problem: unauthorized access to cpu memory.
- Flaw is introduced in the 90ies
- Mitigation: remove/block features introduced to speed up CPU performance
- Since the vulnerability is ”only” mitigated, new exploits may be found

Design Flaw Vulnerabilities

MIT Researchers Discover New Flaw in Apple M1 CPUs That Can't Be Patched.
https://thehackernews.com/2022/06/mit-researchers-discover-new-flaw-in.html

Another Interesting aspect . . . I



Another Interesting aspect . . .

when dealing with vulnerabilities . . . or how to get confronted with Nation State Actor level malware

- WannaCry, ransom worm propagating through EternalBlue exploit (developed by NSA)
- Used a vulnerability only known to NSA.
- NSA "lost" it, . . . somehow
- Someone else used it, worldwide impact (on icrosoft Systems which reached EOL) https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- Follow the money (BitCoin) pointed to North Korea, but well . . .

Vulnerabilities in systems that reached EOL

Operating systems are on very different timescales then . . .

- Service devices used in public transport.
- Systems used in SMEs without dedicated IT support units.
- Systems that control: large medical devices, CNC machines (Mechanical departement), Lab devices (spectrometers and such)
- Discussion: How to protect these?

Vulnerabilities in systems that reached EOL

Operating systems are on very different timescales then . . .

- Service devices used in public transport.
- Systems used in SMEs without dedicated IT support units.
- Systems that control: large medical devices, CNC machines (Mechanical departement), Lab devices (spectrometers and such)
- Discussion: How to protect these?
- $\rightarrow$ These devices including the threats to them are identified in an Risk Assessment

Are systems that reached EOL a CSIRT Problem?

Depends, if there is a policy that EOL systems are not allowed (to be connected to the network), yes, . . . but if the policy only requires to react to critical vulnerabilities better stay away . . . and wait for a critical vulnerability in the beyond EOL system..

Vulnerabilities with low impact to your own infra

Consider vulnerabilities that do not have an impact on the service availability for example in in your dns resolver, memecached, ntp-server.
Should we take care of that?

DRDOS and LINX

Side effects: about a bullet proof hoster and spamhaus dispute (2013)

- Spamhaus puts cyberbunker on their blacklist
- cyberbuner attacks spamhaus (DRDOS) (spamhouse down)
- cloudflare helps spamhouse.
- cyberbunker increased the attack, 300GbpsS peak, LINX down

Distributed Reflection DOS

Distributed Reflection Denial of Service attack No need for a botnet, just use existing servers with UDP services.

- Some services can be misused because they amplify the request: DNS, NTP, SNMP, ...1 small query in, 1 large answer out
- This misuse can be avoided by disabling specific options or implementing firewall rules. Typical amplification factors
  - DNS: ≈50-100
  - NTP: ≈500-5000
  - SNMP: ≈6-12

Patches were AVAILABLE, problem solved?

Distributed Reflection DOS

Distributed Reflection Denial of Service attack No need for a botnet, just use existing servers with UDP services. No!

- 2018 memecached vulnerability
- amplification factor: 51.200
- 1.3 Tbps (twice of what was achieved with the mirai botnet in 2017

QnA

Thanks for your attention, Questions?