

# Vulnerability Management

S. Gabriel<sup>1,2</sup>

<sup>1</sup>Nikhef    <sup>2</sup>EGI CSIRT

April 2025



# Vulnerability Management

# 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 Risk management 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 lot devices (with googable default passwords).

# Vulnerability Lifecycle

The time from vulnerability 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!

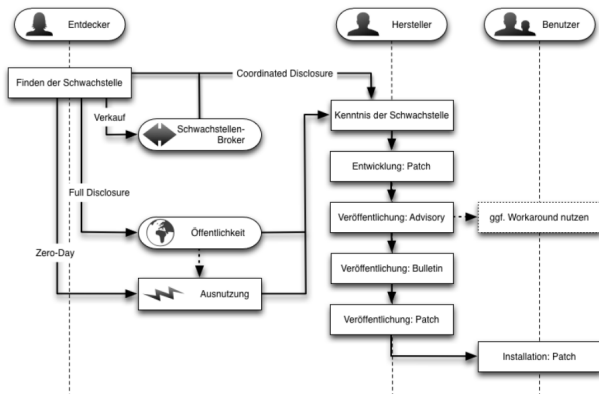
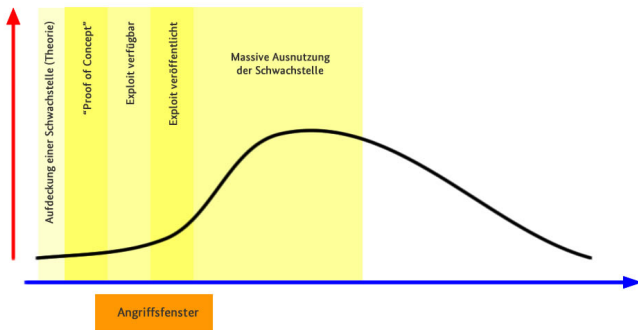


Abbildung 1: Lebenszyklus einer Schwachstelle

# Vulnerability, urgency for patching

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

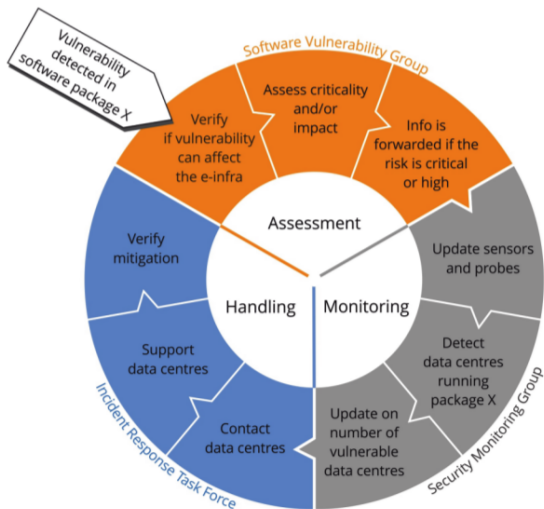


2

<sup>2</sup><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. <sup>3</sup>
- ▶ Criticality is often expressed as a numerical value resulting from the assessment using CVSS <sup>4</sup>
- ▶ Other Specifications, Tools: CPE (Common Platform Enumeration), CWE (Common Weakness Enumeration), dictionary.)
- ▶ machine readable (xml), format: cpe:/ hardware-part [ OS-part [ / application-part ] ]

---

<sup>3</sup><https://cve.mitre.org/>

<sup>4</sup><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 management.

- ▶ Management Board approved procedure
- ▶ Secure service operation policies

# Vulnerability handling in action

## Patch Status monitoring: Local root exploit:

**SECURITY DASHBOARD** HOME

Y --any--

Test Name	Test status	Detection age	Site	Service	flags	info
Pakli-Vuln CRITICAL - Found following unresolved vulnerabilities in Pakli: one-2015-0225	critical	319	RRC-KI	[REDACTED]		<a href="#">info</a>
Pakli-Vuln CRITICAL - Found following unresolved vulnerabilities in Pakli: one-2015-0225	critical	319	ATLAND	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	TUDresden-ZIH	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	IR-IPM-HEP	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	CESGA	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	Kharkov-KIPT-LCG2	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	TRIGRID-INFN-CATANIA	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	IFCA-LCG2	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	IL-TAU-HEP	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	UNICAN	[REDACTED]		<a href="#">info</a>
Pakli-Check	critical	319	RECAS-NAPOLI	[REDACTED]		<a href="#">info</a>

[https://operations.portal.ed.eu/cs/SecurityDashboard/issue/cvbnod0554e3839f1de467\\_73695991/html/tab/overview/page/issues](https://operations.portal.ed.eu/cs/SecurityDashboard/issue/cvbnod0554e3839f1de467_73695991/html/tab/overview/page/issues)

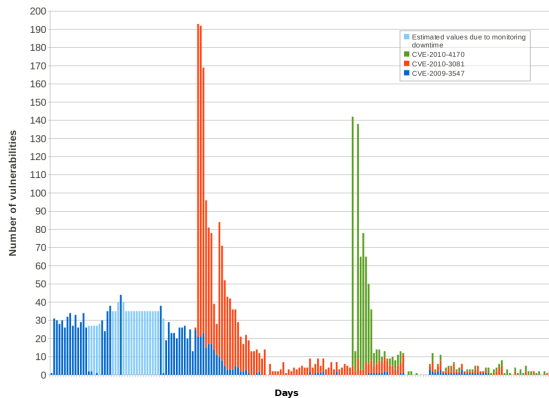
# Vulnerability handling in progress

- ▶ Advisories send to Resource Centres  
<https://advisories.egi.eu/>
- ▶ 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?

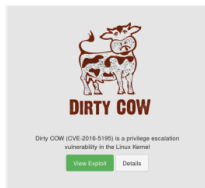
# Vulnerability handling in action



Hm, not really ...

# Vulnerabilities with Icons I

Interesting vulnerabilities got names ...and icons.



# Vulnerabilities with Icons II

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

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

```
p.....#.....g  
zip,deflate....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: mumblemumbleum.ac.uk..DNT: 1..Connection: Keep-Alive  
e..Authorization: Basic cm9vdDpnYXpYWfHYZ2I=....
```

10/14

# Vulnerabilities with Icons II

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

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

p.....#.....g
zip,deflate....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-Alive
e..Authorization: Basic cm9vdDpnYXpYWfhYZ2I=....

>>> base64.b64decode("cm9vdDpnYXpYWfhYZ2I=")
'root:gazXXXgb'
```

10/14

# 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 ...!

The image shows a train schedule on the left and a ransomware payment screen on the right. The train schedule lists routes such as Friedberg - Gießen, F-Süd - Offenbach, and F-Süd - Hanau, along with estimated travel times and delays. The ransomware screen, titled 'Wanna Decryptor 2.0', displays a message: 'Oops, your files have been encrypted!' and asks for a Bitcoin payment of \$300 to decrypt the files. It includes a countdown timer for the payment deadline and a Bitcoin address for the payment.

Route	Approx. Time	Retardation
Friedberg - Gießen	25 min.	environ 25 min.
Friedberg - Gießen	38 min.	5 min. - environ 5 min.
F-Süd - Offenbach	38 min.	5 min. - environ 5 min.
F-Süd - Hanau	42 min.	prox. 20 min. - environ 20 min.

**Wanna Decryptor 2.0**

**Oops, your files have been encrypted!**

**Was geschah mit meinem Computer?**  
Ihre wichtigen Dateien sind verschlüsselt. Viele Ihrer Dokumente, Fotos, Videos, Datenbanken und andere Dateien sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Vielleicht sind Sie damit beschäftigt, einen Weg zu finden, um Ihre Dateien wiederherzustellen, aber verschwenden Sie nicht Ihre Zeit. Niemand kann Ihre Dateien ohne unseres Entschlüsselungsdienst wiederherstellen.

**Kann ich meine Dateien wiederherstellen?**  
Sicher. Wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber du hast nicht genug Zeit. Sie können einige Ihrer Dateien kostenlos entschlüsseln. Versuchen Sie jetzt, indem Sie auf <Decrypt> klicken. Aber wenn du alle deine Dateien entschlüsseln willst, musst du bezahlen. Sie haben nur 3 Tage, um die Zahlung einzureichen. Danach wird der Preis verdoppelt. Auch wenn du nicht in 7 Tagen bezahlt hast, kannst du deine Dateien nicht für immer wiederherstellen. Wir haben freie Veranstaltungen für Besitzer, die so arm sind, dass sie nicht in 6 Monaten bezahlen können.

**Wie bezahle ich?**  
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf <About bitcoin>.

**Send \$300 worth of bitcoin to this address:**  
119p7UMMngoJ1pMvkpHjcrdJNOj6rLn

**Check Payment**      **Decrypt**

## 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 Microsoft Systems which reached EOL) [https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](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?
- ▶ → 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
- ▶ cyberbunker attacks spamhaus (DRDOS) (spamhouse down)
- ▶ cloudflare helps spamhouse.
- ▶ cyberbunker increased the attack, 300Gbps 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:  $\approx 50-100$
  - ▶ NTP:  $\approx 500-5000$
  - ▶ SNMP:  $\approx 6-12$

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)