Vulnerability Management

S. Gabriel[1,2]

[1]Nikhef [2]EGI CSIRT

Sept. 2026

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.”

Vulnerabiity Management in EGI

EGI: Advanced Computing for a Data-Driven Future[1]

[1] https://www.egi.eu/

EGI CSIRT Operational Security I

What we do:

- Provide an EGI federation-wide security monitoring capability
- Correlate events across members to detect multi-member campaigns that no single member could detect alone
- Maintain a central view on federation-wide threat activity
- Produce EGI federation-wide situational awareness reports for governance and members
- Cross-EGI-member incident coordination — managing communication between affected members without breaching confidentiality
- Crisis coordination — activating federation-wide response for major incidents
- Post-incident review and across EGI members Resource Centers — identifying systemic weaknesses

EGI CSIRT Operational Security II

What we don't do:

- EGI CSIRT does not handle member-internal incidents — those stay with the member (but we do provide (forensics) support on request).
- Replace EGI member Resource Center Security Operations — we supplement/support we do not substitute this function at the EGI members Resource Center level

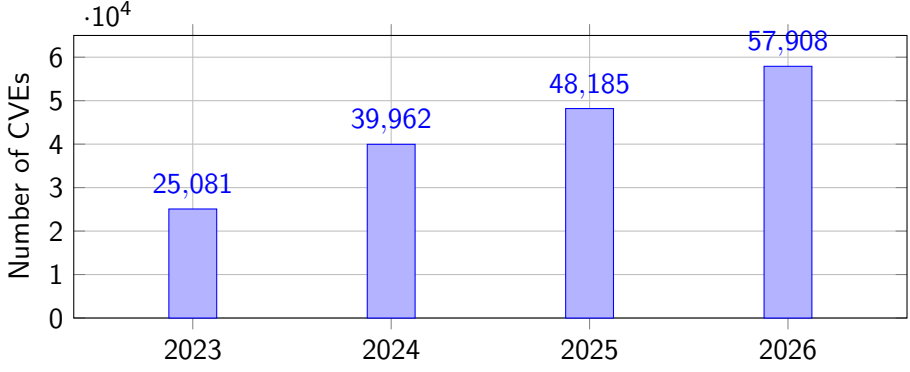
Where AI enters the IT Security Domain

AI stirs up IT Security Risk Management

Risk Analysis Phase; Risk calculation:

$$Risk = Impact * Likelihood$$

- Impact, numerical value determined in the Primary Asset Valuation step,Business Impact Analysis
- Likelihood: =f(EASINESS + POWER + INTEREST)

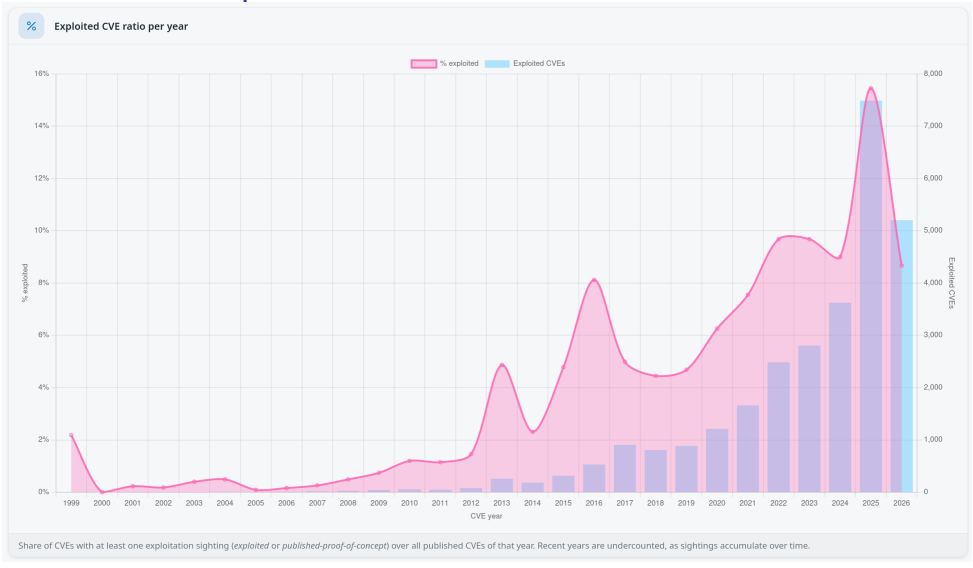


number of CVEs/year: 2026 value is year-to-date through 31 August 2026.

What does this mean, and what are we in control of

- Number of vulnerabilities go up significantly, is our current process able to keep up?
- We cannot control the number of vulnerabilities, but we can optimize our processes and use AI for time consuming steps.
- Is the current estimate on threat actor capability still valid? probably not.

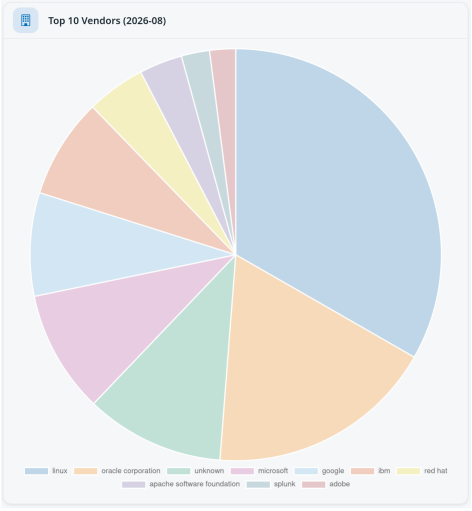
Exploited CVE Ratio per Year



[2] CIRCL https://www.vulnerability-lookup.org/

2*

Not a problem of a particular vendor



[3]CIRCL `https://www.vulnerability-lookup.org/`

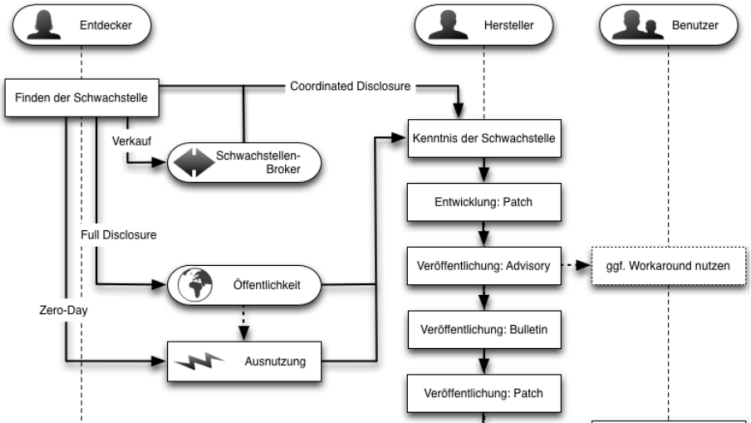
[3]*

Scope: Vulnerability Management in EGI

- We (EGI) are a Linux shop, Microsoft does things differently, will not be discussed here.
- EGI backoffice infra is out of scope and under responsibility of EGI
- 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).

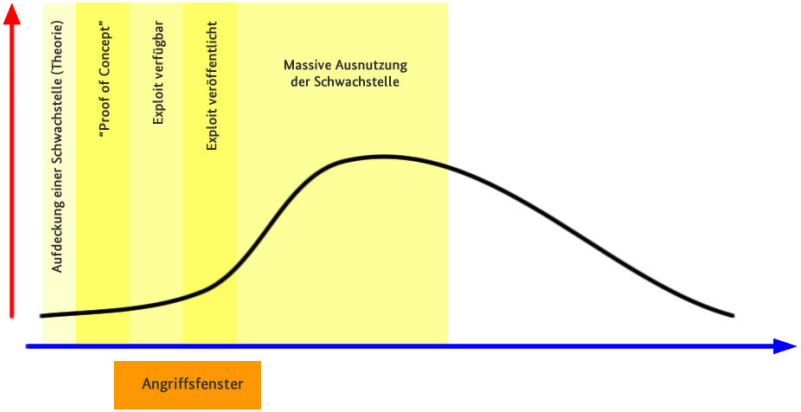
Vulnerability Lifecycle

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!



Vulnerability, urgency for patching

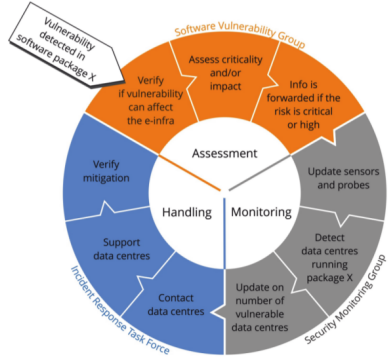
Urgent action is required for: Vulnerabilities (assessed as critical by EGI) **and** for which an exploid is published.



[5] https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/

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 ...

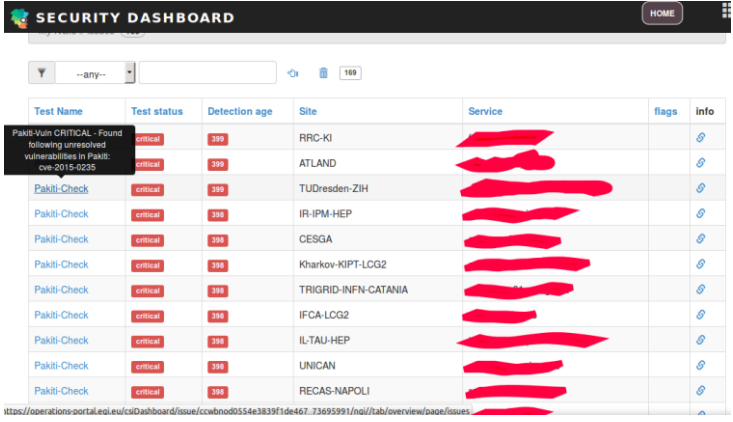
Vulnerability handling, Policies

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 service operation policies

Vulnerability handling in action

Patch Status monitoring: Local root exploit:



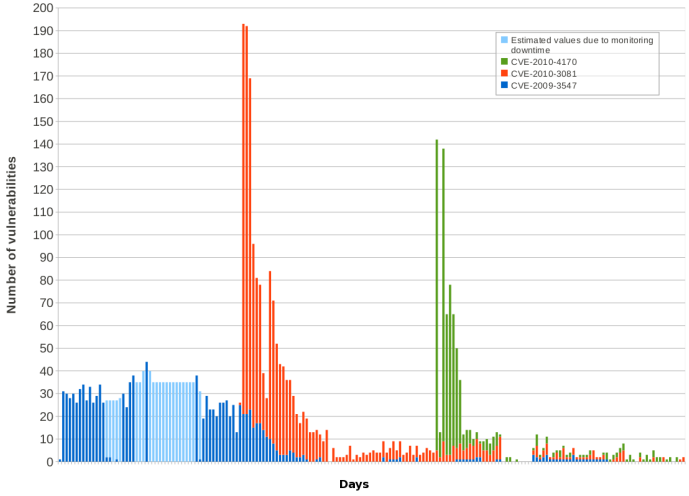
Vulnerability handling in progress

- 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?

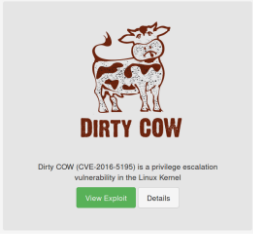
Vulnerability handling in action



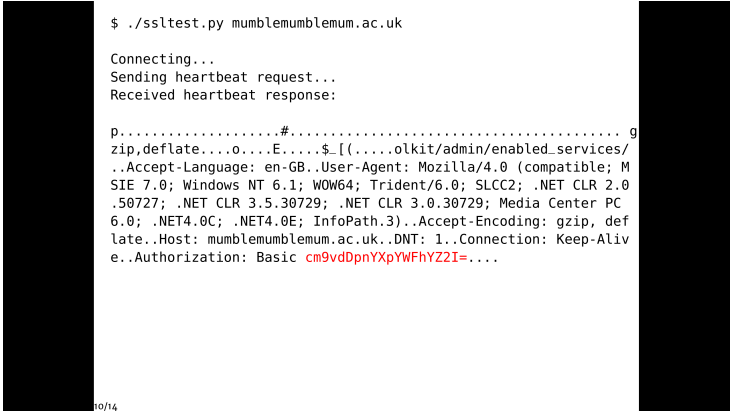
Hm, not really ….

Vulnerabilities with Icons I

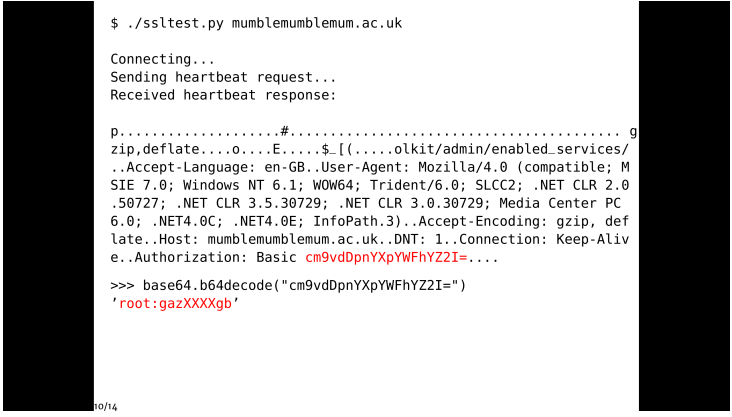
Interesting vulnerabilities got names ...and icons.



Vulnerabilities with Icons II



Vulnerabilities with Icons II



Design Flaw Vulnerabilities

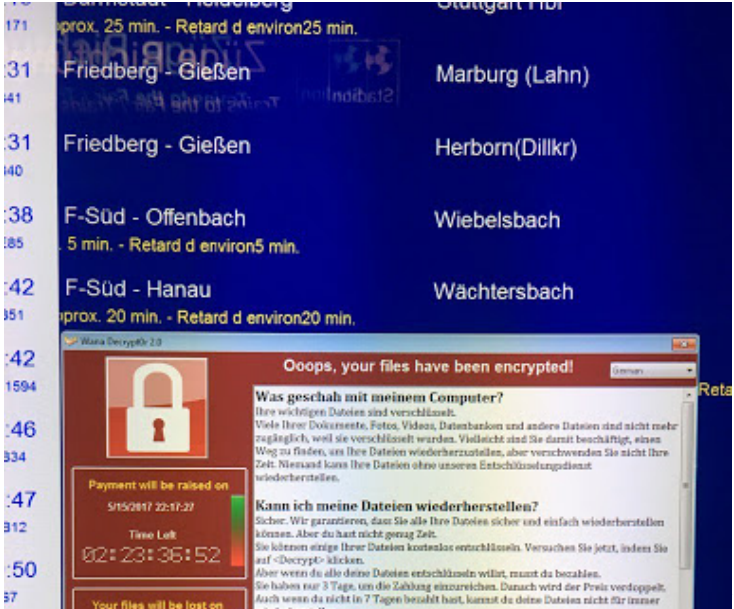
Meltdown and Spectre:

- 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