Workshop:
Securing the Embedded World: Effective Testing

Cyber Security Vlaanderen/Flanders
KU LEUVEN DistriNet
VUB

Workshop:
Securing the Embedded World: Effective Testing

Agenda:

10:15 - 10:30: Welcome Coffee
10:30 - 10:35: Introduction (J. Lapon, KUL)
10:35 – 11:00: Strengths and Pitfalls of Embedded Security Testing Tools (J. Lapon, KUL)
11:00 - 11:25: Exposing Remote Access Risks: A WebRTC Analysis Framework (V. Goeman, KUL)
11:25 - 11:50: Onweer: Automated Resilience Testing through Fuzzing (G. Coremans, VUB)
11:50 - 12:00: Discussion

VLAIO/COOCK:

BUGATTI -Embedded Security Testing and Automation

Partners and User group

VLAIO

DistriNet gent:

SOFTWARE LANGUAGES LAB

Atlas Copco

Belden

COMmeto

KAUTZ.IO

COLRUYT GROUP

CTRL engineering

FORCEBIT® measurement made easy

TÜV AUSTRIA BELGIUM

GemOne

guestway™

hydroko

spotit YOUR SECURITY & NETWORK LAYER

Invisto

PSICONTROL for high-tech breakthroughs

QUICKSAND

Secudea

TELEDYNE FLIR Everywhereyoulook™

televic GSP

VersaSense Industrial Edge Intelligence

savaco IT's about impact

WYGWAM niko

zensor

TOREON Business driven cyber consulting

.AGORIA

CYBER SECURITY COALITION.be

VLAIO Coock

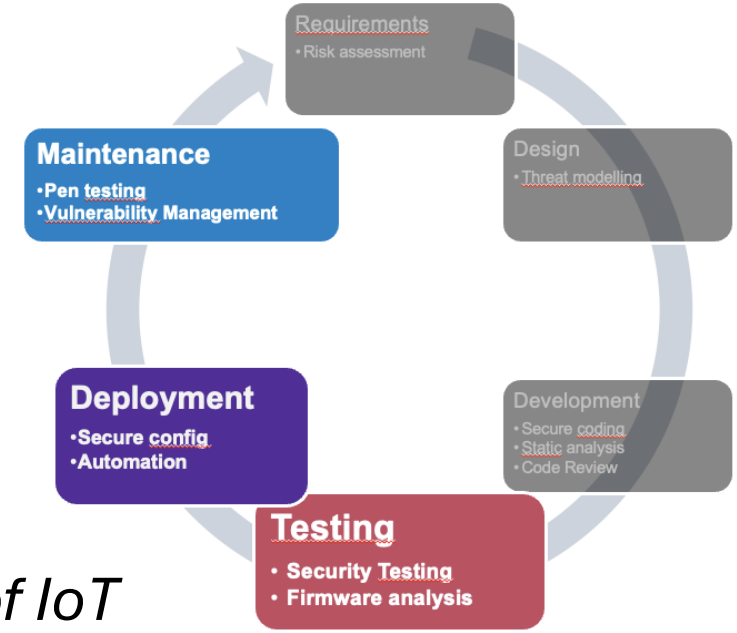
- *Collective R&D and Knowledge dissemination*
- 3 years (since April 1st)
- user group meetings (3/year)
- hands-on seminars/workshops

- Goal: Integration in ‘your’ organization

Goals

Security testing of IoT applications

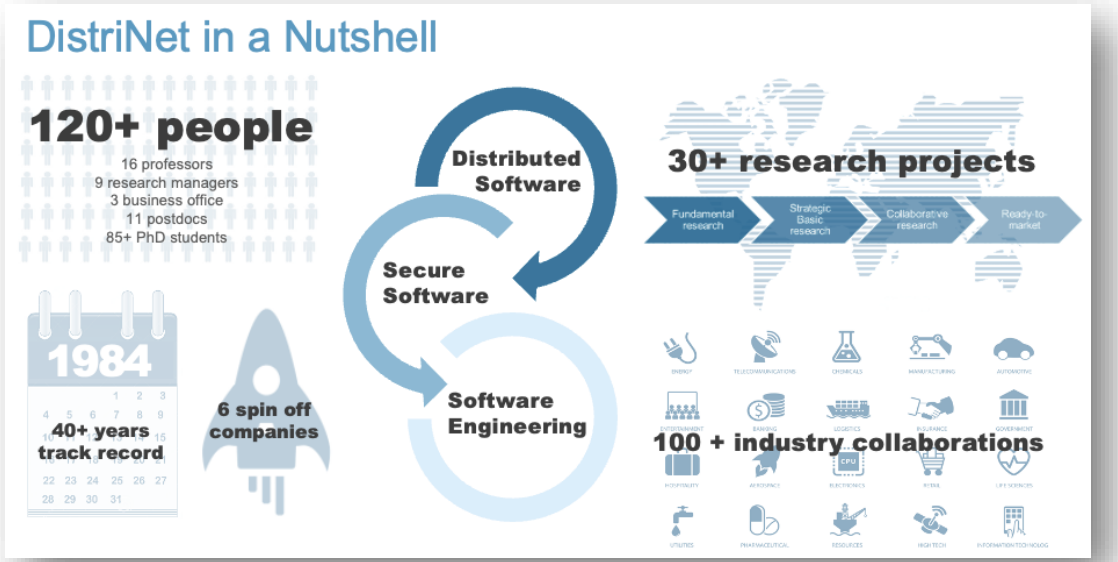
- *Tools for static analysis of device firmware*
- *Advanced dynamic/pen-testing techniques*



Secure configuration, deployment and management of IoT

- *Infrastructure as code*
- *Attack detection, security-orchestration and incident response*

DistriNet gent:



gent:

- Embedded Security
  detection, mitigation, handling, compliance, legislation…
- Privacy Enhancing Technologies
  anonymization, controlled release and retention of sensitive data…
- System security
  multi-variant execution, memory vulnerability mitigations…

Cyber Security Vlaanderen/Flanders

KU LEUVEN DistriNet VUB

SOFTWARE LANGUAGES LAB

Coen De Roover

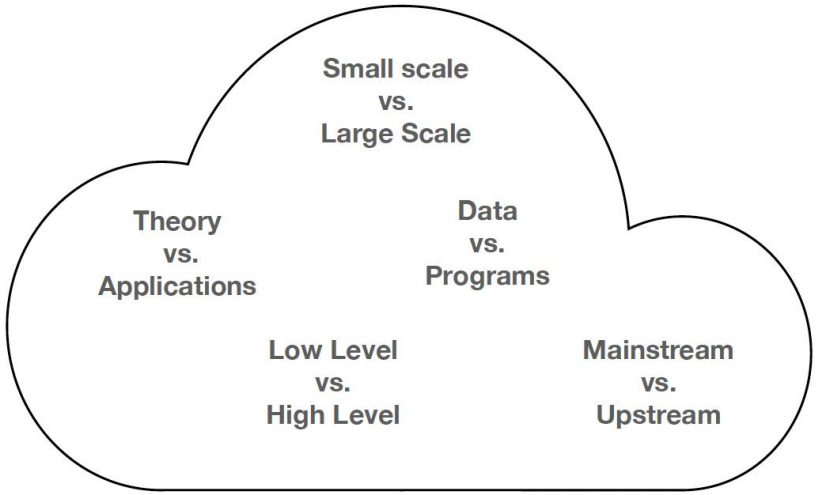
2015

program analysis
design and
applications in
software quality

Jens Nicolay

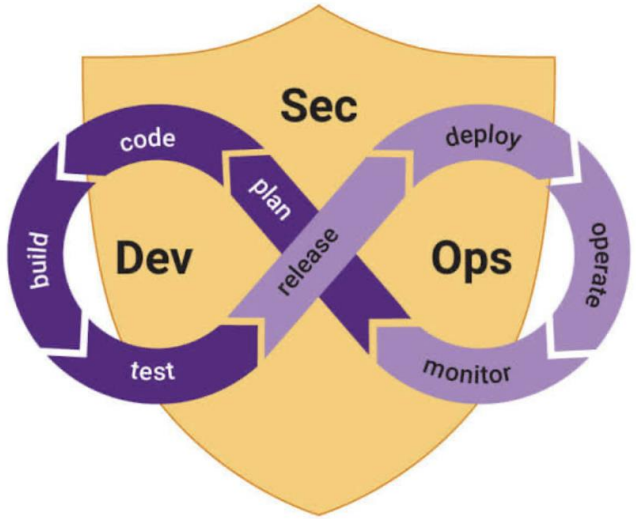
2024

applied software
research,
reactive security



Research Diversity Dimensions at SOFT

“ SOFT researches **theories**, **technologies** and **methods** that are at the basis of, or help to improve, the **construction** **of** **software** at all layers of the **software stack** that **begins** where **computer engineering ends** and **goes up** to and includes **application construction**. ”



- empirical research into **secure practices**
- **reactive security** & incident management
- dynamic and static program **analyses**
- **tools** for SCA, SAST, DAST, IAST, RASP
- secure programming **abstractions**
- secure programming **languages**

Cyber Security Vlaanderen/Flanders

KU LEUVEN DistriNet

VUB

Workshop:
Securing the Embedded World: Effective Testing

Agenda:

10:15 - 10:30: Welcome Coffee
10:30 - 10:35: Introduction (J. Lapon, KUL)
10:35 – 11:00: Strengths and Pitfalls of Embedded Security Testing Tools (J. Lapon, KUL)
11:00 - 11:25: Exposing Remote Access Risks: A WebRTC Analysis Framework (V. Goeman, KUL)
11:25 - 11:50: Onweer: Automated Resilience Testing through Fuzzing (G. Coremans, VUB)
11:50 - 12:00: Discussion

Cyber Security Vlaanderen/Flanders
KU LEUVEN DistriNet VUB

Strengths and Pitfalls of Embedded Security Testing Tools

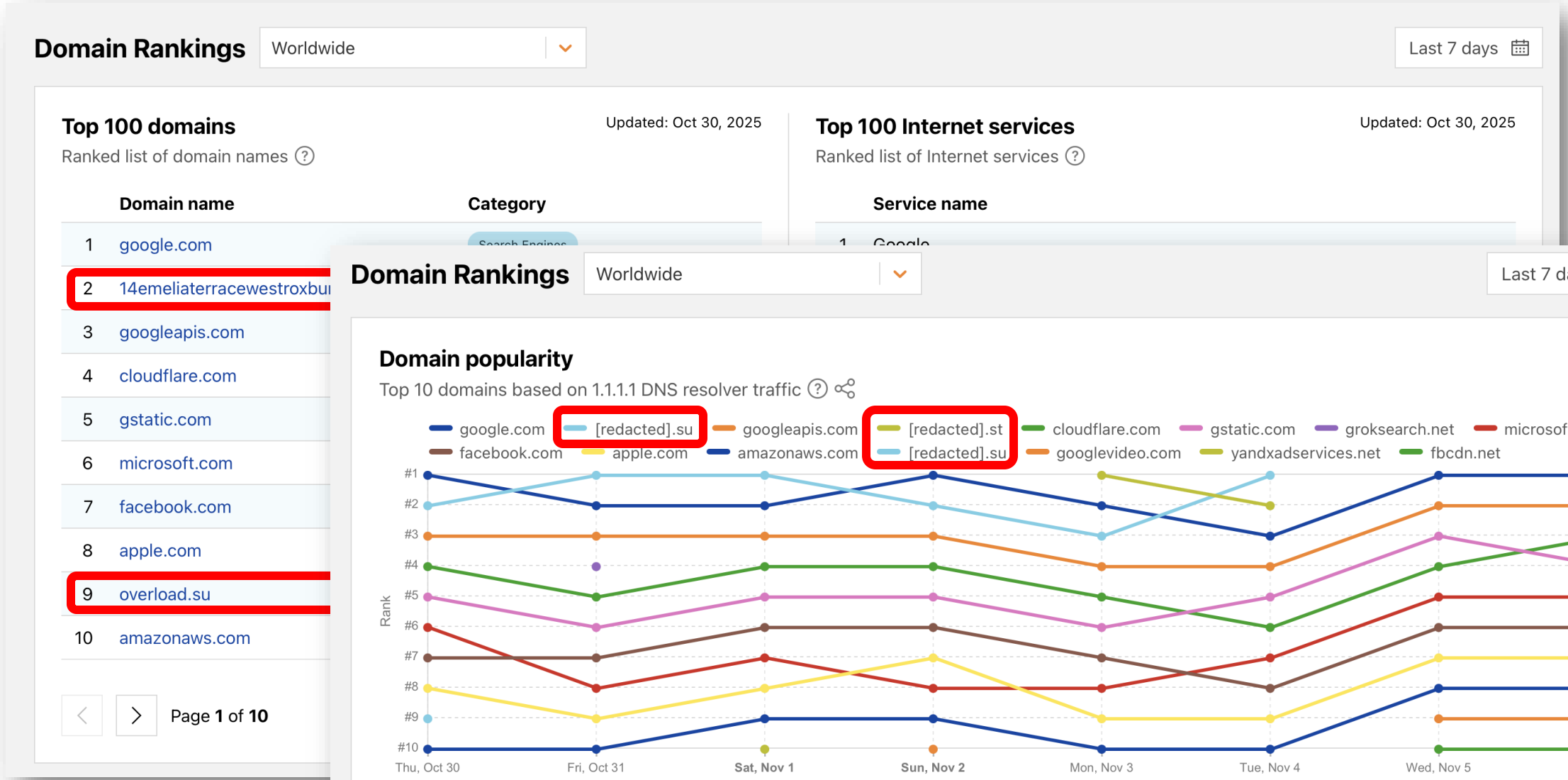
From CVE Overload to Actions

Jorn Lapon

Cyber Security Vlaanderen/Flanders
KU LEUVEN DistriNet VUB

Why Embedded Security Testing Matters

AISURU botnet
Residential Proxy Abuse



http://radar.cloudflare.com

Cyber Security Vlaanderen/Flanders

KU LEUVEN DistriNet VUB

Why Embedded Security Testing Matters

Akira ransomware

Ransomware gang encrypted network from a webcam to bypass EDR

By **Bill Toulas** March 6, 2025 03:31 PM 5

The Akira ransomware gang was spotted using an unsecured webcam to launch encryption attacks on a victim's network, effectively circumventing Endpoint Detection and Response (EDR), which was blocking the encryptor in Windows.

Cybersecurity firm S-RM team discovered the unusual attack method during a recent incident response at one of their clients.

Notably, Akira only pivoted to the webcam after attempting to deploy encryptors on Windows, which were blocked by the victim's EDR solution.

Why Embedded Security Testing Matters

EU regulations (CRA, RED-DA,…) now make

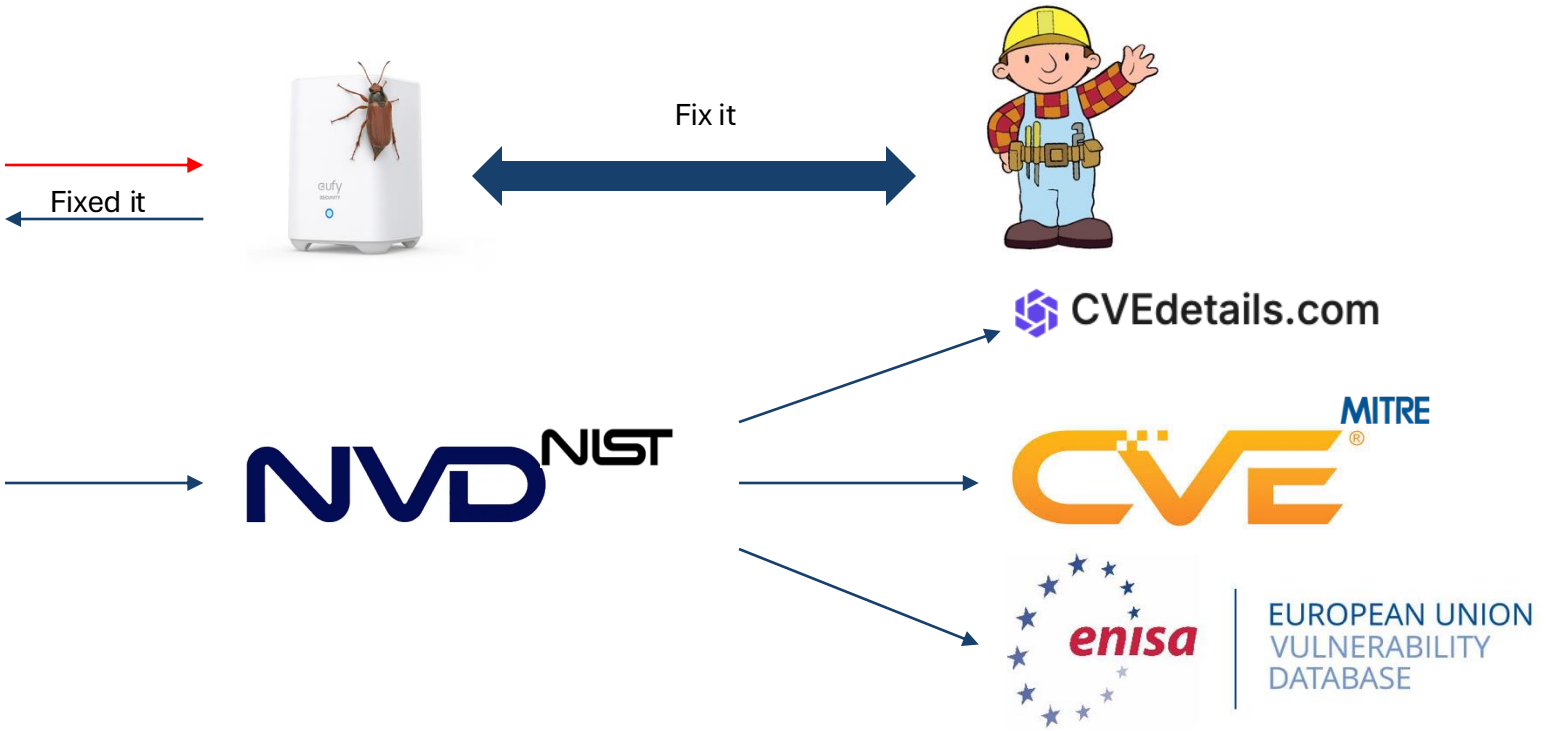
security testing mandatory for your products.

Types of Embedded Security Tools

Category	Purpose	Input	Examples
SAST (Static Application Security Testing)	find coding flaws, memory issues	**source code**	cppcheck, clang-tidy, flawfinder
DAST (Dynamic Application Security Testing)	trigger unexpected behavior/exploits	**running/emulated applications**	AFL, CI Fuzz, Aikido DAST, …
SCA (Software Composition Analysis)	known vulnerabilities (CVEs)	dependency **manifests, SBOMs**	Grype, Snyk, (build-tools)
Network Scanners	(DAST style) fingerprinting to infer versions and CVEs	**network**-exposed endpoints of running/emulated system	Nmap, Nessus, OpenVAS
Configuration/Hardening Analysis	check how software and OS are built and configured	**image config**, **file system**	Lynis, OpenSCAP, Yocto Security Flags
Firmware Analysis	Combines binary extraction and vulnerability scanning	**firmware/binary blobs**	EMBA, FACT
… many more …			

Known Vulnerabilities

- CVE – Common Vulnerabilities and Exposures
  - CVE-2023-37822 – responsible disclosure



Known Vulnerabilities – CVEs Everywhere

- CVE – Common Vulnerabilities and Exposures
  - CVE-2023-37822

Vulnerability Details : CVE-2023-37822

Eufy Homebase 2 Predictable WPA2-PSK Allows Offline Brute Force and Unauthorized Network Access

The Eufy Homebase 2 before firmware version 3.3.4.1h creates a dedicated wireless network for its ecosystem, which serves as a proxy to the end user's primary network. The WPA2-PSK generation of this dedicated network is flawed and solely based on the serial number. Due to the flawed generation process, the WPA2-PSK can be brute forced offline within seconds. This vulnerability allows an attacker in proximity to the dedicated wireless network to gain unauthorized access to the end user's primary network. The only requirement of the attack is proximity to the dedicated wireless network.

Products affected by CVE-2023-37822

Anker » Eufy Homebase 2 Firmware » Version: 3.2.8.3h
cpe:2.3:o:anker:eufy_homebase_2_firmware:3.2.8.3h:*:*:*:*:*:*:* — Matching versions

Eufy » Homebase 2 Firmware Versions before (<) 3.3.4.1h
cpe:2.3:o:eufy:homebase_2_firmware:*:*:*:*:*:*:*:* — Matching versions
When used together with: Eufy » Homebase 2 » Version: N/A

Exploit prediction scoring system (EPSS) score for CVE-2023-37822

EPSS FAQ

0.06% Probability of exploitation activity in the next 30 days EPSS Score History

~ 19 % Percentile, the proportion of vulnerabilities that are scored at or less

CVSS scores for CVE-2023-37822

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
8.2	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N	2.8	4.7	134c704f-9b21-4f2e-91b3-4a467353bcc0	2024-11-25
8.2	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N	2.8	4.7	NIST	2024-10-29

Great, we can find out what software and libraries are vulnerable and we need to patch!

So what’s the problem?

We found **critical** vulnerabilities
CVE-XXXX, CVE-YYYY, CVE-ZZZZ in your device!

Fix them?

Your Customer

Security Dashboard

Device	135 Critical CVEs	227 High CVEs	156 Medium CVEs

Vulnerabilities Over Time

Top Vulnerabilities

Critical

High

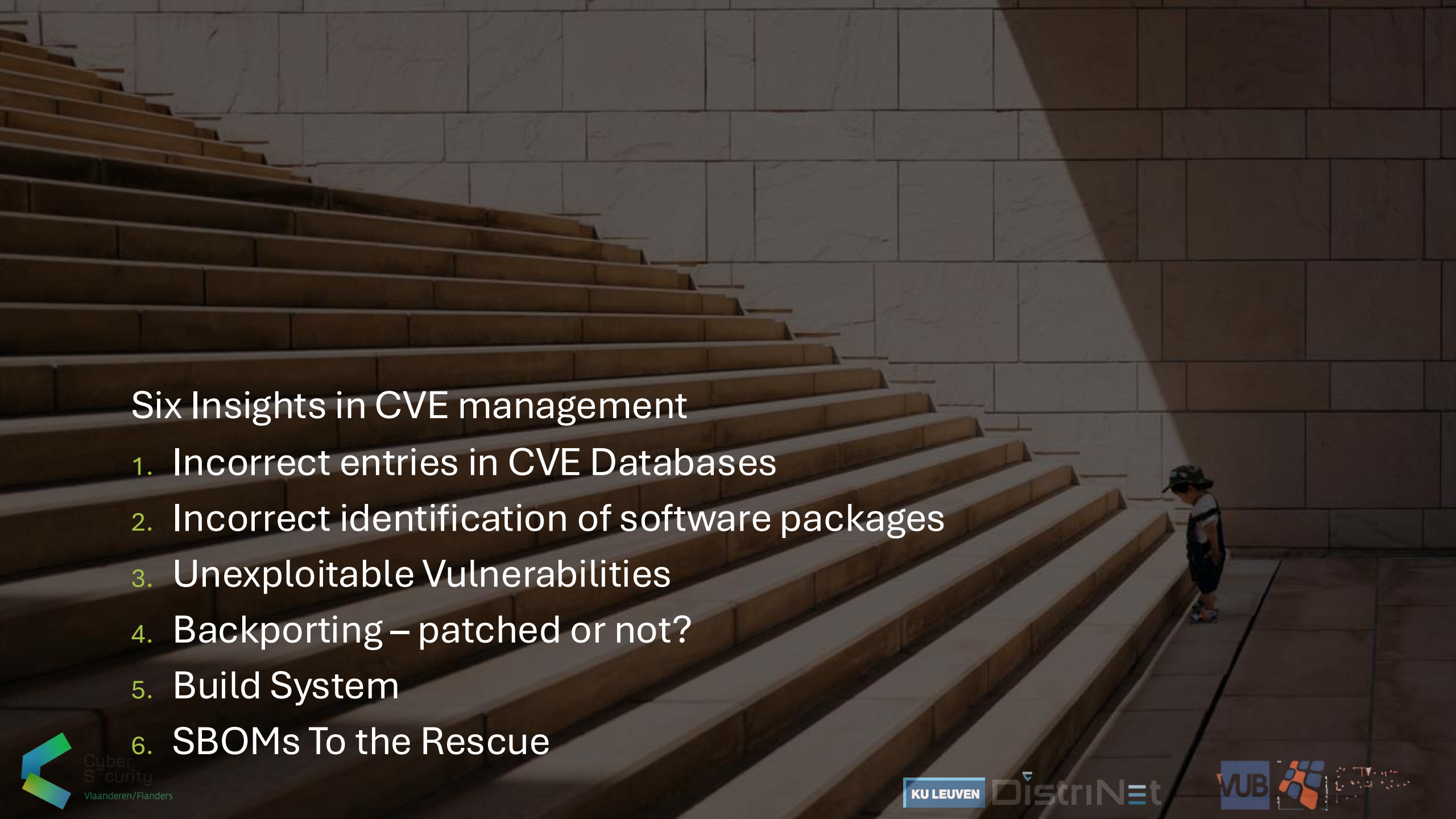
Medium

Severity Distribution

Medium

Critical High Medium

Recent Activity

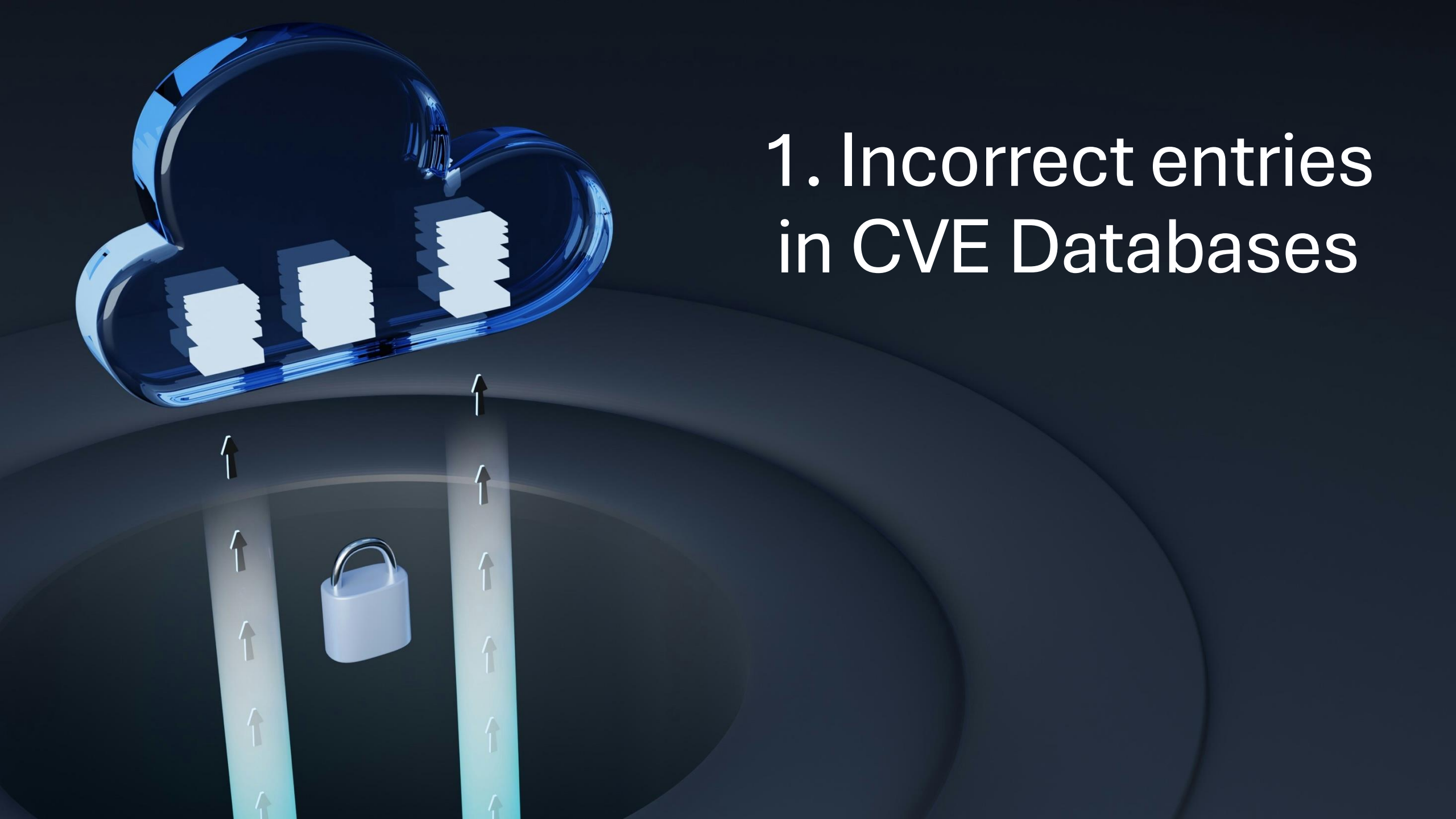


Six Insights in CVE management

1. Incorrect entries in CVE Databases
2. Incorrect identification of software packages
3. Unexploitable Vulnerabilities
4. Backporting – patched or not?
5. Build System
6. SBOMs To the Rescue

Cyber Security Vlaanderen/Flanders

KU LEUVEN DistriNet VUB



1. Incorrect entries in CVE Databases

CVE-2023-37822 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

The Eufy Homebase 2 before firmware version 3.3.4.1h creates a dedicated wireless network for its ecosystem, which serves as a proxy to the end user's primary network. The WPA2-PSK generation of this dedicated network is flawed and solely based on the serial number. Due to the flawed generation process, the WPA2-PSK can be brute forced offline within seconds. This vulnerability allows an attacker in proximity to the dedicated wireless network to gain unauthorized access to the end user's primary network. The only requirement of the attack is proximity to the dedicated wireless network.

QUICK INFO

CVE Dictionary Entry:
CVE-2023-37822
NVD Published Date:
10/03/2024
NVD Last Modified:
11/25/2024
Source:
MITRE

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NVD	**NIST:** NVD	**Base Score:** 8.2 HIGH	**Vector:** CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N
	ADP: CISA-ADP	**Base Score:** 8.2 HIGH	**Vector:** CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

CVE-2023-37822 PUBLISHED

View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: MITRE Corporation

Published: 2024-10-03 **Updated:** 2024-10-04

Description

The Eufy Homebase 2 before firmware version 3.3.4.1h creates a dedicated wireless network for its ecosystem, which serves as a proxy to the end user's primary network. The WPA2-PSK generation of this dedicated network is flawed and solely based on the serial number. Due to the flawed generation process, the WPA2-PSK can be brute forced offline within seconds. This vulnerability allows an attacker in proximity to the dedicated wireless network to gain unauthorized access to the end user's primary network. The only requirement of the attack is proximity to the dedicated wireless network.

Product Status

Learn more

Information not provided

References 4 Total

- http://anker.com

EUVD-2023-41696

Back to the vulnerability search

Severity

EPSS Score **0.06** %

Alternative IDs

CVE-2023-37822
GSD-2023-37822

Summary

The Eufy Homebase 2 before firmware version 3.3.4.1h creates a dedicated wireless network for its ecosystem, which serves as a proxy to the end user's primary network. The WPA2-PSK generation of this dedicated network is flawed and solely based on the serial number. Due to the flawed generation process, the WPA2-PSK can be brute forced offline within seconds. This vulnerability allows an attacker in proximity to the dedicated wireless network to gain unauthorized access to the end user's primary network. The only requirement of the attack is proximity to the dedicated wireless network.

Affected Product

Vendor:	Product:	Version:
n/a	n/a	n/a

Advisory IDs 0

Vulnerability information

Published: 2024-10-03 00:00 **Updated:** 2024-11-25 21:15 **Assigner:** mitre

References

http://anker.com
http://eufy.com
https://www.usenix.org/conference/woot24/presentation/goeman
https://www.usenix.org/system/files/woot24-goeman.pdf

1. Incorrect entries in CVE Databases

CVE-2024-6604 Detail

Description

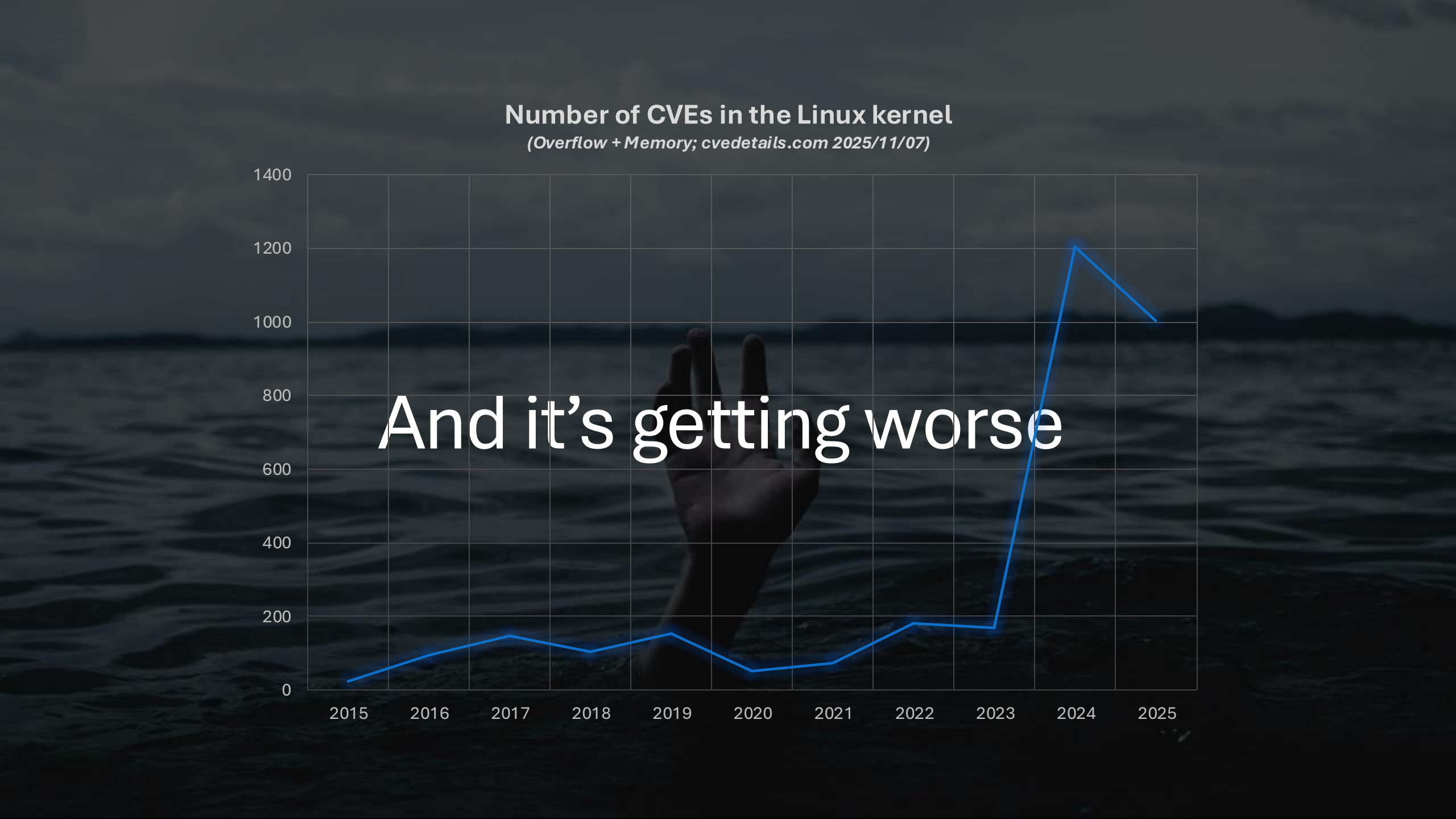
Memory safety bugs present in Firefox 127, Firefox ESR 115.12, and Thunderbird 115.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:mozilla:firefox:*:*:*:*:esr:*:*:* Show Matching CPE(s)	Up to (excluding) 115.13	
cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:* Show Matching CPE(s)	Up to (excluding) 126.0	
cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:* Show Matching CPE(s)	Up to (excluding) 115.13	
cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:* Show Matching CPE(s)	From (including) 116.0	Up to (excluding) 128.0

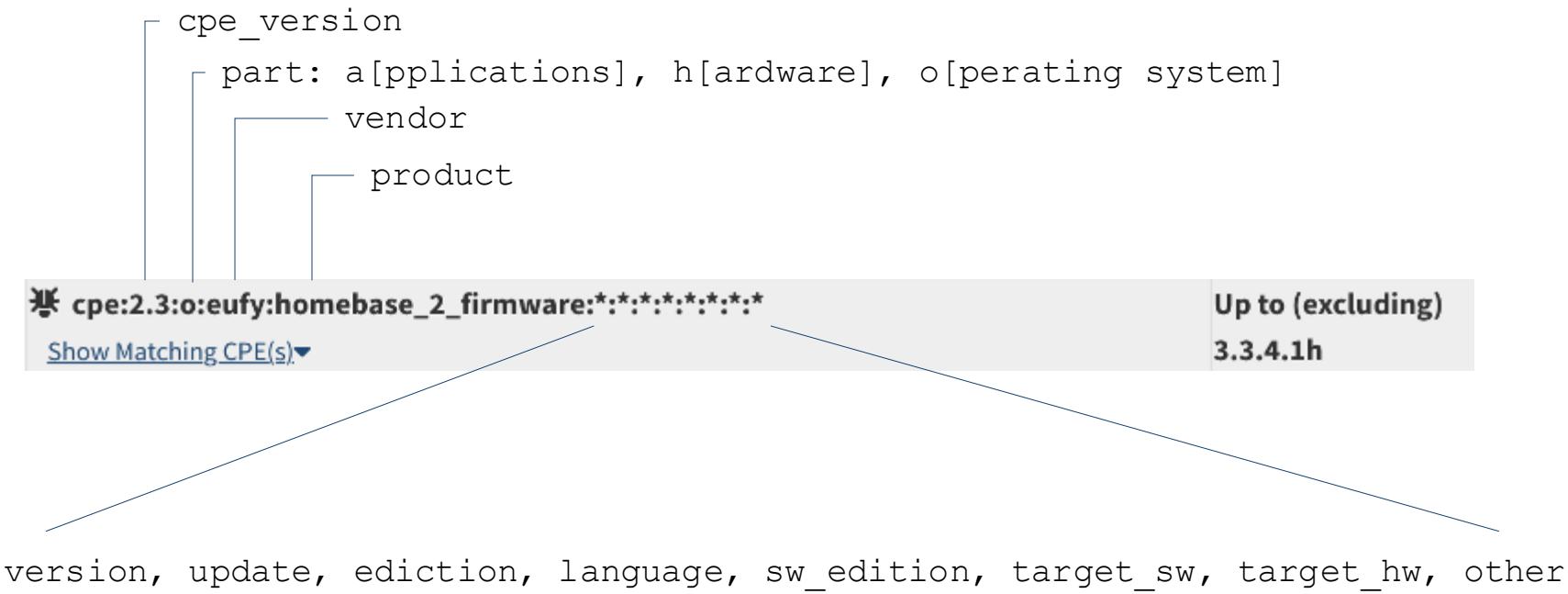
https://nvd.nist.gov/vuln/detail/cve-2024-6604


Number of CVEs in the Linux kernel
(Overflow + Memory; cvedetails.com 2025/11/07)
1400
1200
1000
800
600
400
200
0
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
And it’s getting worse

2. Incorrect Identification of Software packages

2. Incorrect Identification of Software Packages

1. **Name + version**
2. **CPE – Common Platform Enumeration – naming scheme**



2. Incorrect Identification of Software Packages

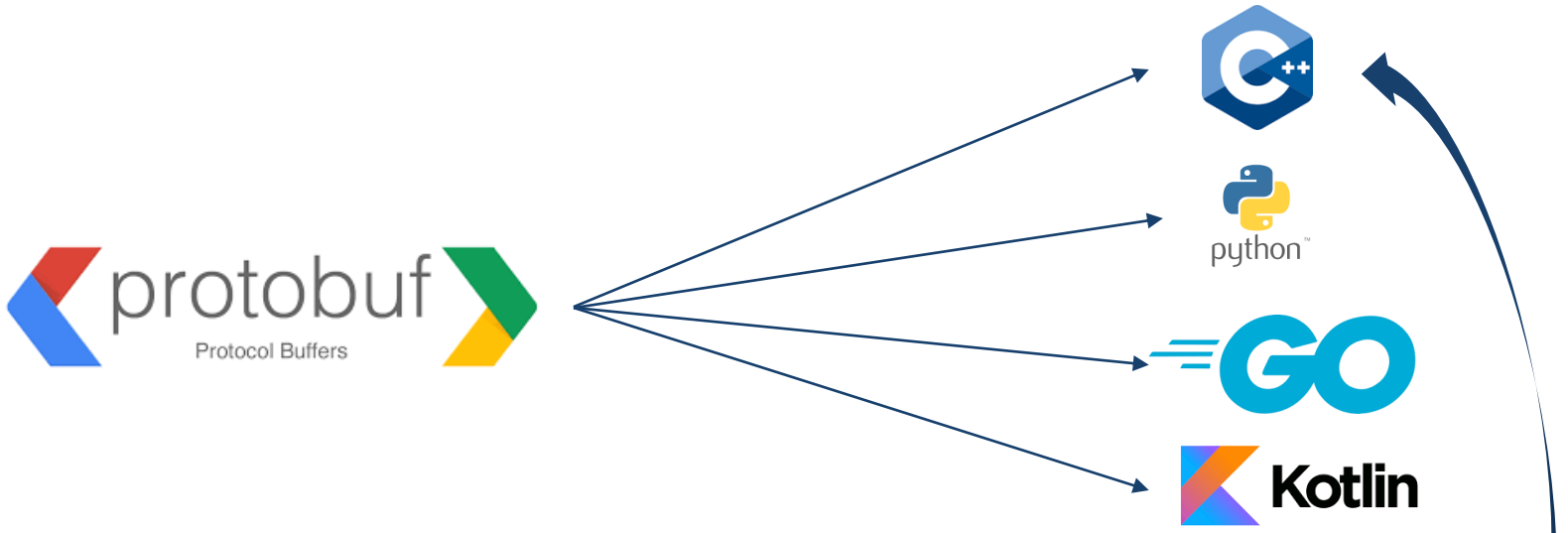
- **Exact identifiers**:
  - From *manifest files, package managers and SBOMs*

Sometimes 'near' exact:
- Package Manager: libxml2@2.9.14
- NVD CPE: cpe:2.3:a:**xmlsoft**:libxml2:2.9.14

- **Heuristic identification**:
  - fingerprints & headers (Network Scanners)
  - regex/string matching (binary analysis, firmware tools)

Often failures in identification:
- Wrong software **package**
- Partial or wrong **version**

2. Incorrect Identification of Software Packages



CVE-2021-22570 Detail

Description

Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file's name during generation of the resulting error message. Since the symbol is incorrectly parsed, the file is nullptr. We recommend upgrading to version 3.15.0 or greater.

3. Unexploitable Vulnerabilities

False Positive … for now

3. Unexploitable Vulnerabilities

CVE-2024-53104 Detail

Description

In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Skip parsing frames of type UVC_VS_UNDEFINED in uvc_parse_format This can lead to out of bounds writes since frames of this type were not taken into account when calculating the size of the frames buffer in uvc_parse_streaming.

= part of UVC Driver (USB Video Class)

kernel module/driver/code
must be present/loaded to be exploitable

3. Unexploitable Vulnerabilities

- Package not present, or vulnerable code not accessible

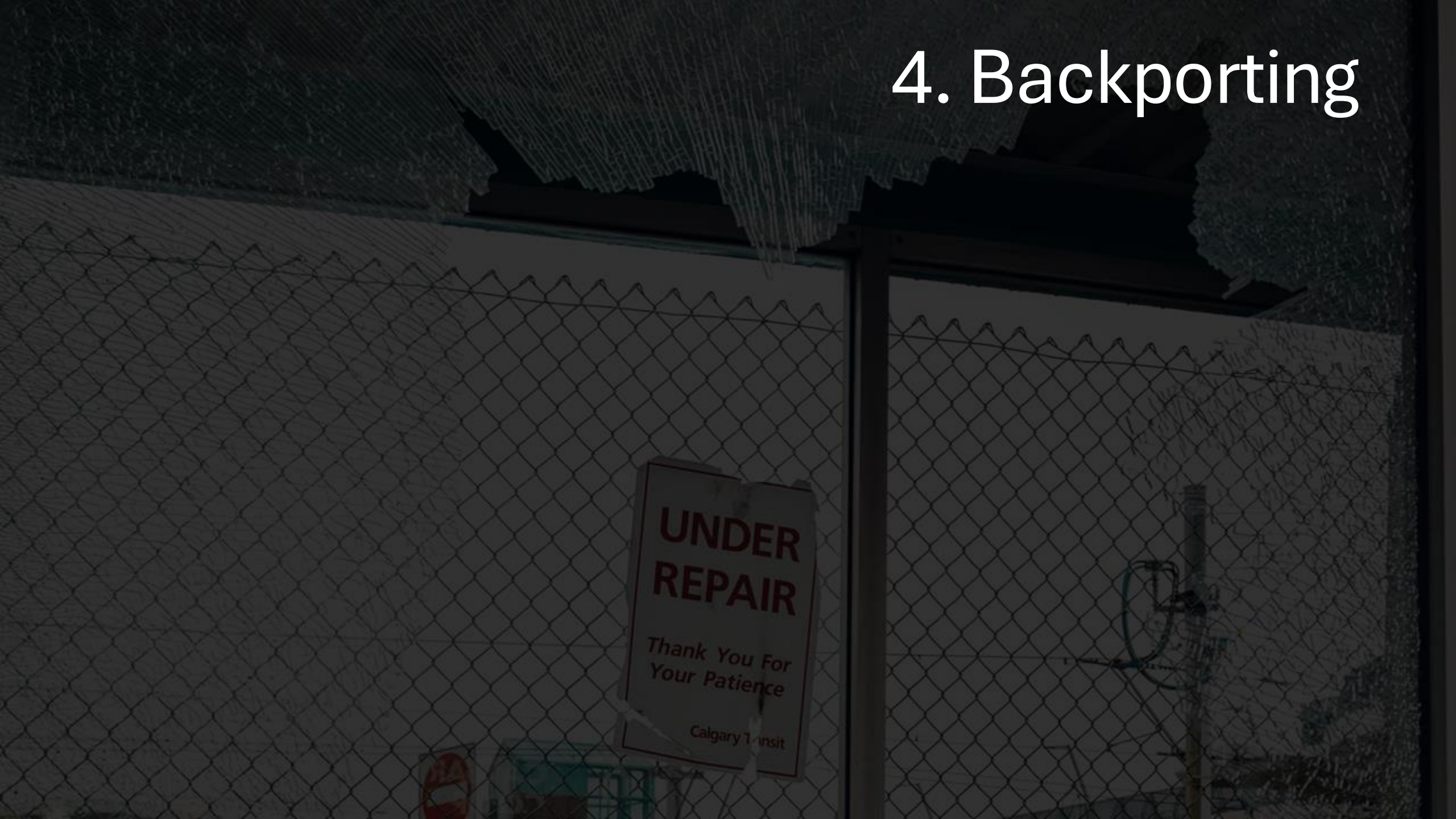
  function not used, module not loaded, #ifdef …

  - Add CVE to ignore list?
  - What if it is used later?

    - ! Make sure that **quietly re-enabling** is not possible !
      - e.g., “nm mybinary | grep vulnerable_function”

    - Document it

4. Backporting

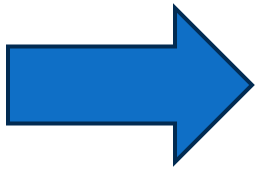


Backporting – patched or not?

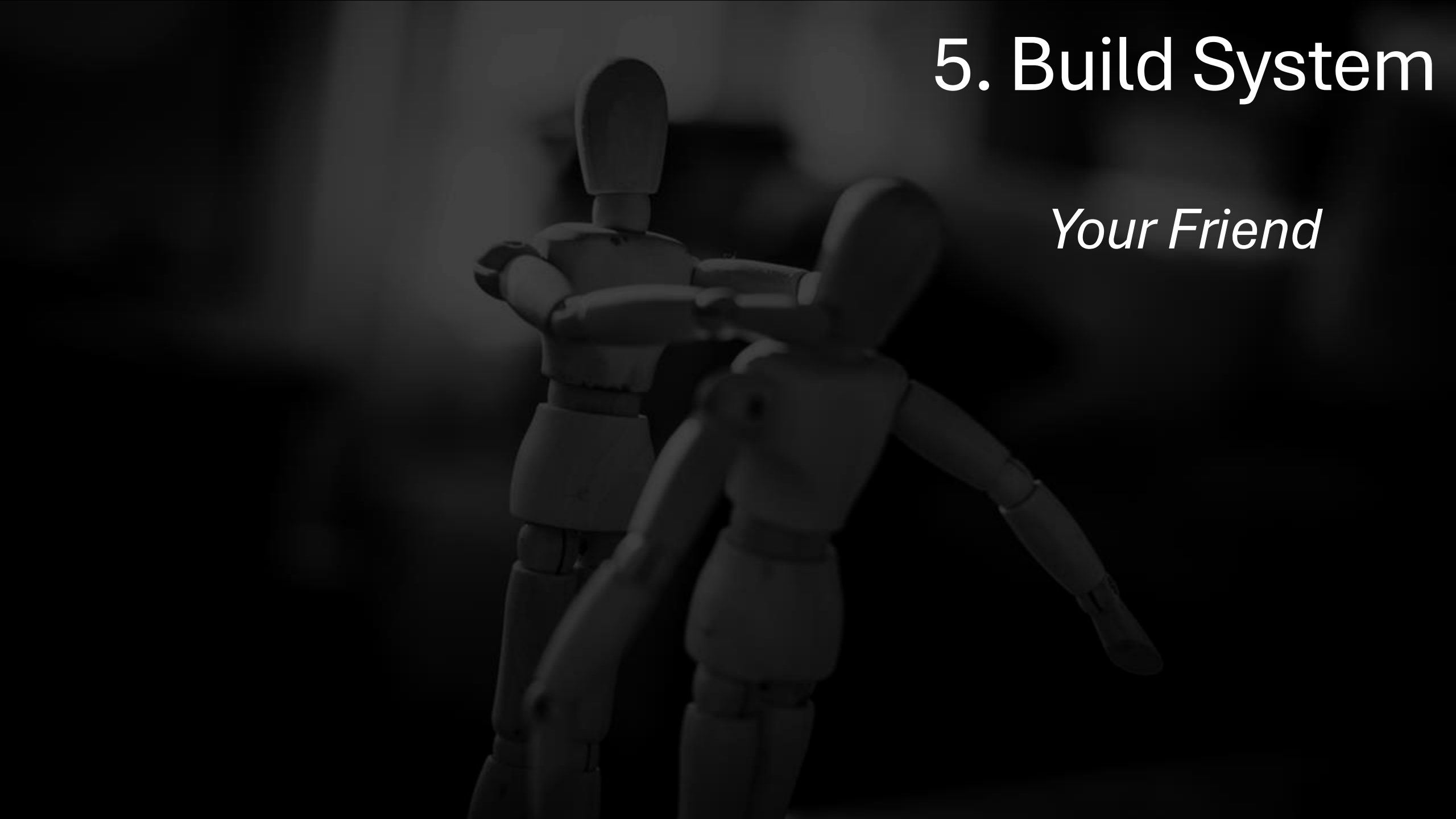
- **Backporting** is the process of porting a software update that was developed for a relatively current version of a software entity, to an older version of the software. [wikipedia]

enterprise and long-term support (LTS) Linux:
Debian, Ubuntu, CentOS, and Red Hat Enterprise Linux (RHEL).

Linux-Yocto, BuildRoot, Vendor BSP layers (TI, NXP, Renesas), ...:
- in built-in layers
- in custom code



CVEs listed may be False Positive (they are patched)



5. Build System

Your Friend

5. Build System

- CVE detection in Yocto and BuildRoot

  - Yocto:
    - cve-check
    - Backporting, false positives: `cve-extra-exclusions.inc`

  - BuildRoot:
    - pkg-stats
    - backporting, false positives: `cve.ignore, cve.fixed`
    - `XXX_IGNORE_CVES` (ignore per package)

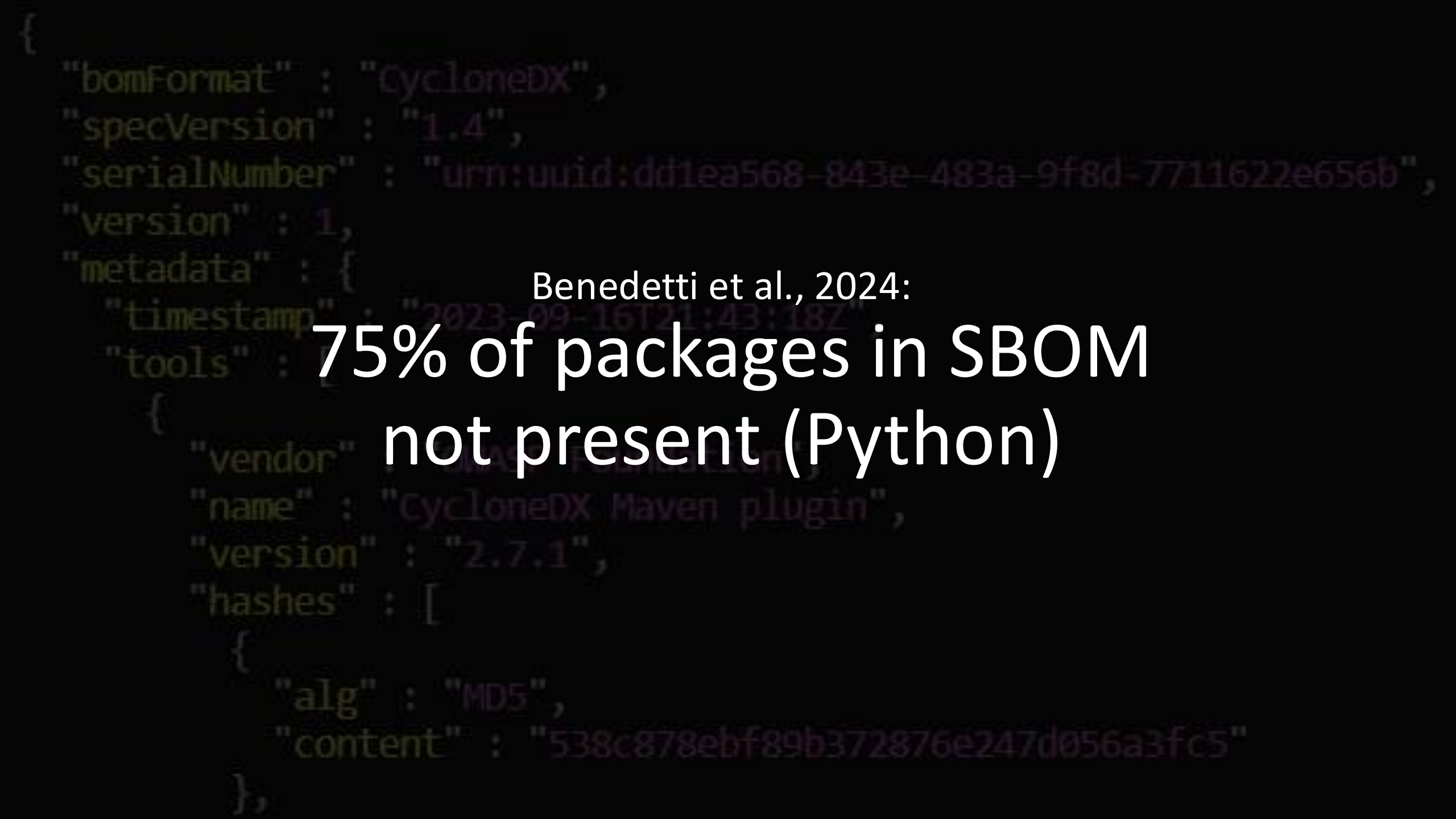
5. Build System

- Build vs Runtime dependencies
- Static libraries not found in Runtime
- Vulnerabilities not detected:
    - *Incorrectly included dependencies (e.g., not added as build package)*
    - *Patched package overwritten with higher layer unpatched package?*
    - *Removed during layered build*
    - *…*

6. SBOMs to the Rescue

or Not?


```
{
  "bomFormat" : "CycloneDX",
  "specVersion" : "1.4",
  "serialNumber" : "urn:uuid:dd1ea568-843e-48
  "version" : 1,
  "metadata" : {
    "timestamp" : "2023-09-16T21:43:18Z",
    "tools" : [
      {
        "vendor" : "OWASP Foundation",
        "name" : "CycloneDX Maven plugin",
        "version" : "2.7.1",
        "hashes" : [
          {
            "alg" : "MD5",
            "content" : "538c878ebf89b372876e247d056a3fc5"
          },
```



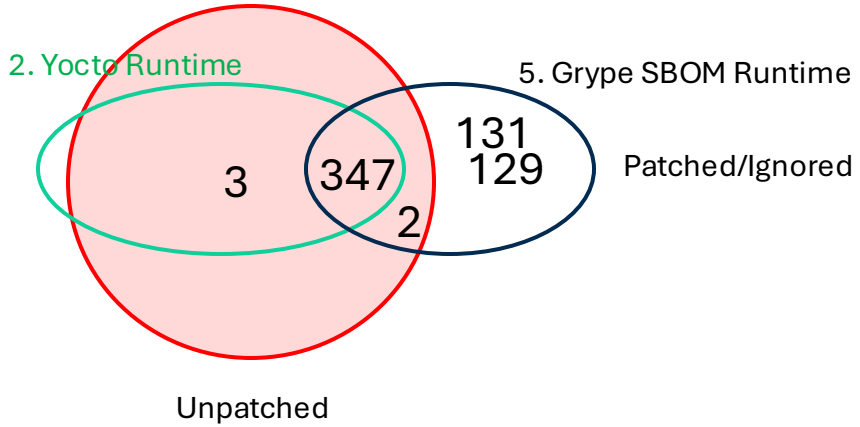
Benedetti et al., 2024:

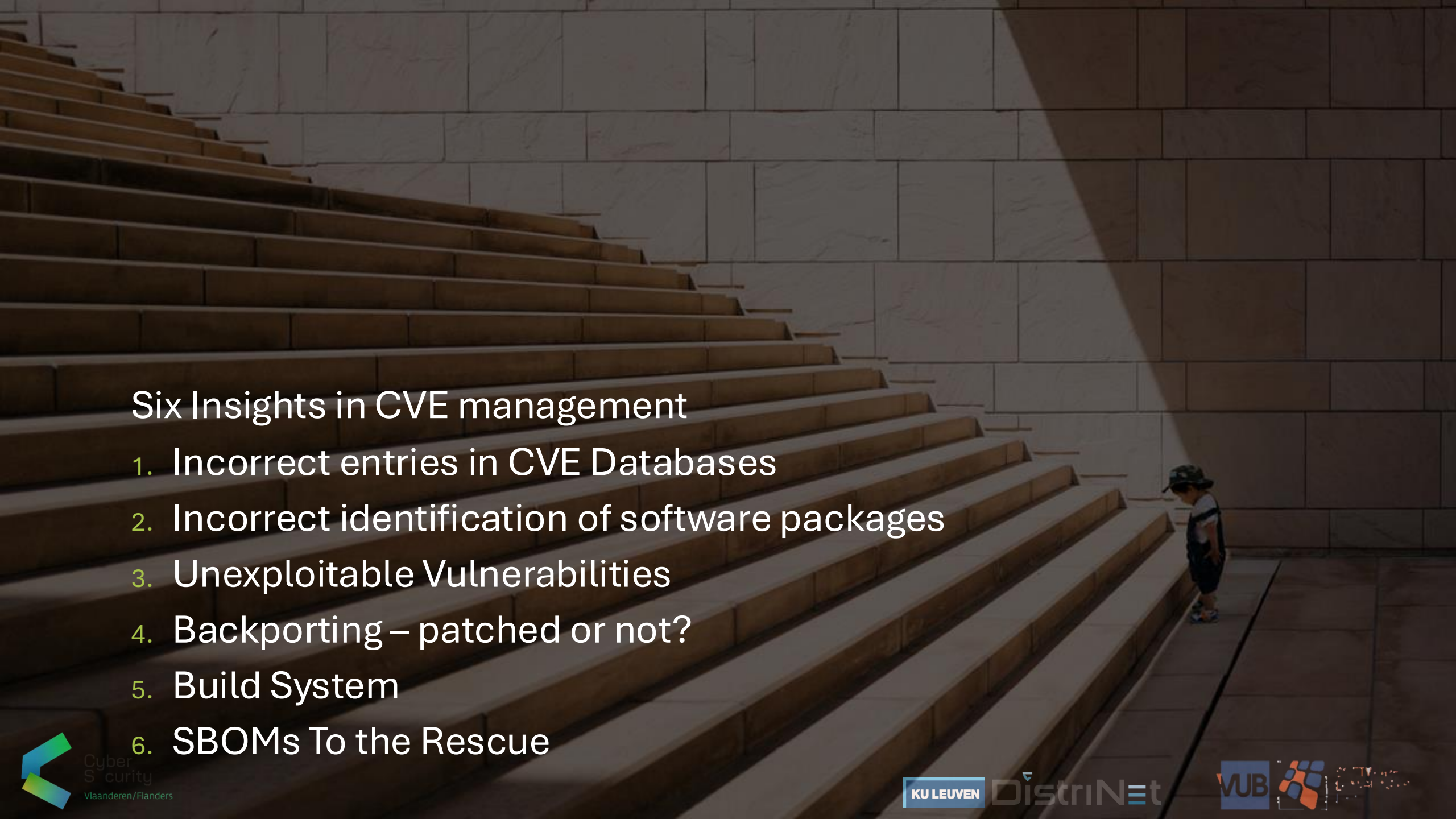
75% of packages in SBOM not present (Python)

6. SBOMs to the Rescue - Experiments

- **Target:** core-image-demo, qemux86-64, Yocto 5.0.13 Scarthgap

	Unpatched CVEs	Vulnerable Packages
1. Yocto	355	glibc libsndfile1 qemu-native kernel





Six Insights in CVE management

1. Incorrect entries in CVE Databases
2. Incorrect identification of software packages
3. Unexploitable Vulnerabilities
4. Backporting – patched or not?
5. Build System
6. SBOMs To the Rescue

Cyber Security Vlaanderen/Flanders

KU LEUVEN DistriNet VUB

Lessons Learned – From CVE Overload to Actions

- Database ≠ Truth
- Fixing ≠ simple patching:
  - *document backports, ignore lists,…*
- Document configuration (modules/drivers/…)
- Build systems already hold truth
- SBOMs are only as smart as their source

Interested in joining Bugatti:
Contact:

Jorn.lapon@kuleuven.be
Coen.De.roover@vub.be

Workshop:
Securing the Embedded World: Effective Testing

Agenda:

10:15 - 10:30: Welcome Coffee
10:30 - 10:35: Introduction (J. Lapon, KUL)
10:35 – 11:00: Strengths and Pitfalls of Embedded Security Testing Tools (J. Lapon, KUL)
11:00 - 11:25: Exposing Remote Access Risks: A WebRTC Analysis Framework (V. Goeman, KUL)
11:25 - 11:50: Onweer: Automated Resilience Testing through Fuzzing (G. Coremans, VUB)
11:50 - 12:00: Discussion

Cyber Security Vlaanderen/Flanders

KU LEUVEN DistriNet VUB

Workshop:
Securing the Embedded World: Effective Testing

Agenda:

10:15 - 10:30: Welcome Coffee
10:30 - 10:35: Introduction (J. Lapon, KUL)
10:35 – 11:00: Strengths and Pitfalls of Embedded Security Testing Tools (J. Lapon, KUL)
11:00 - 11:25: Exposing Remote Access Risks: A WebRTC Analysis Framework (V. Goeman, KUL)
11:25 - 11:50: Onweer: Automated Resilience Testing through Fuzzing (G. Coremans, VUB)
11:50 - 12:00: Discussion

Cyber Security Vlaanderen/Flanders
KU LEUVEN DistriNet VUB