

Securimag

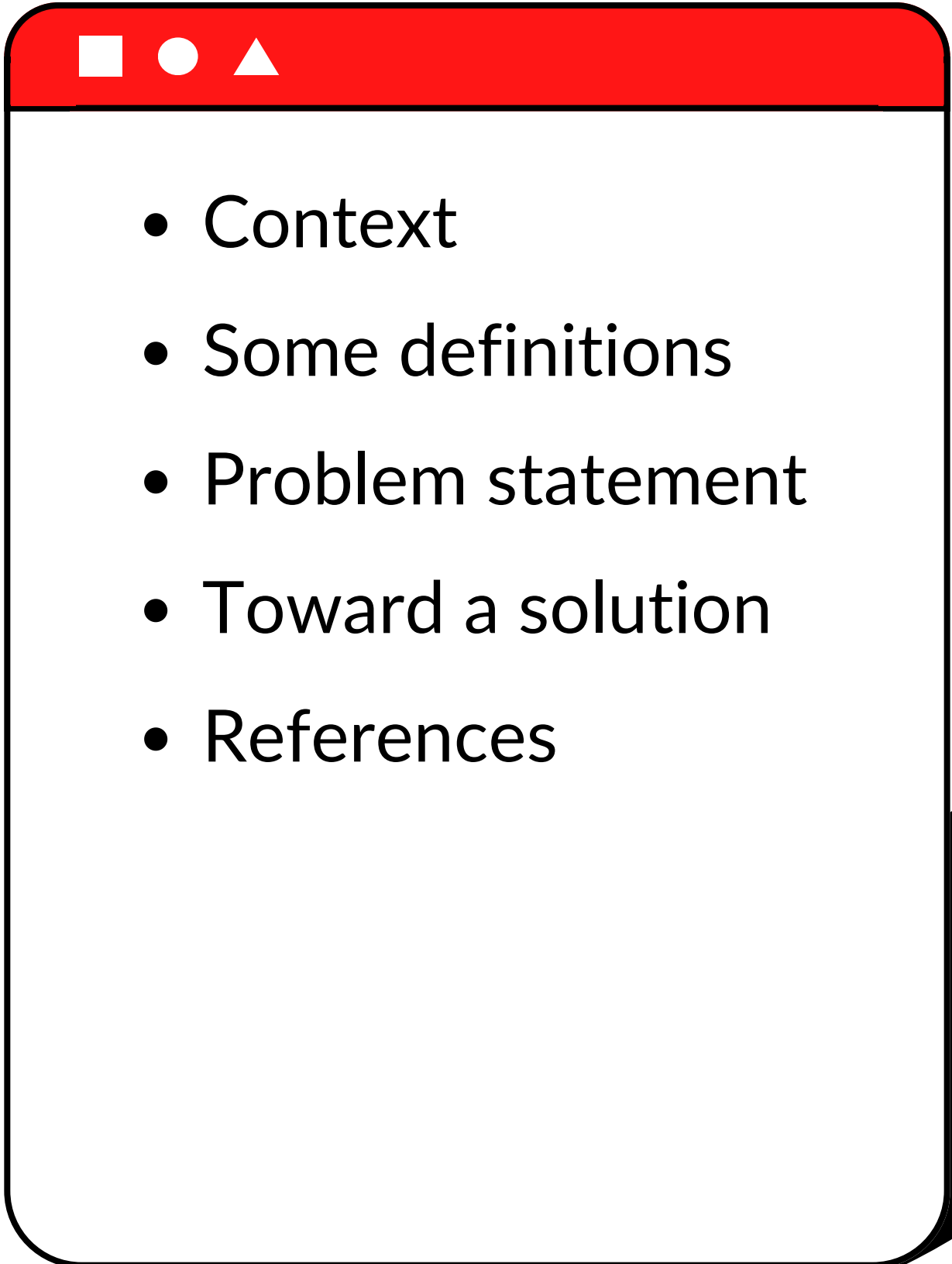
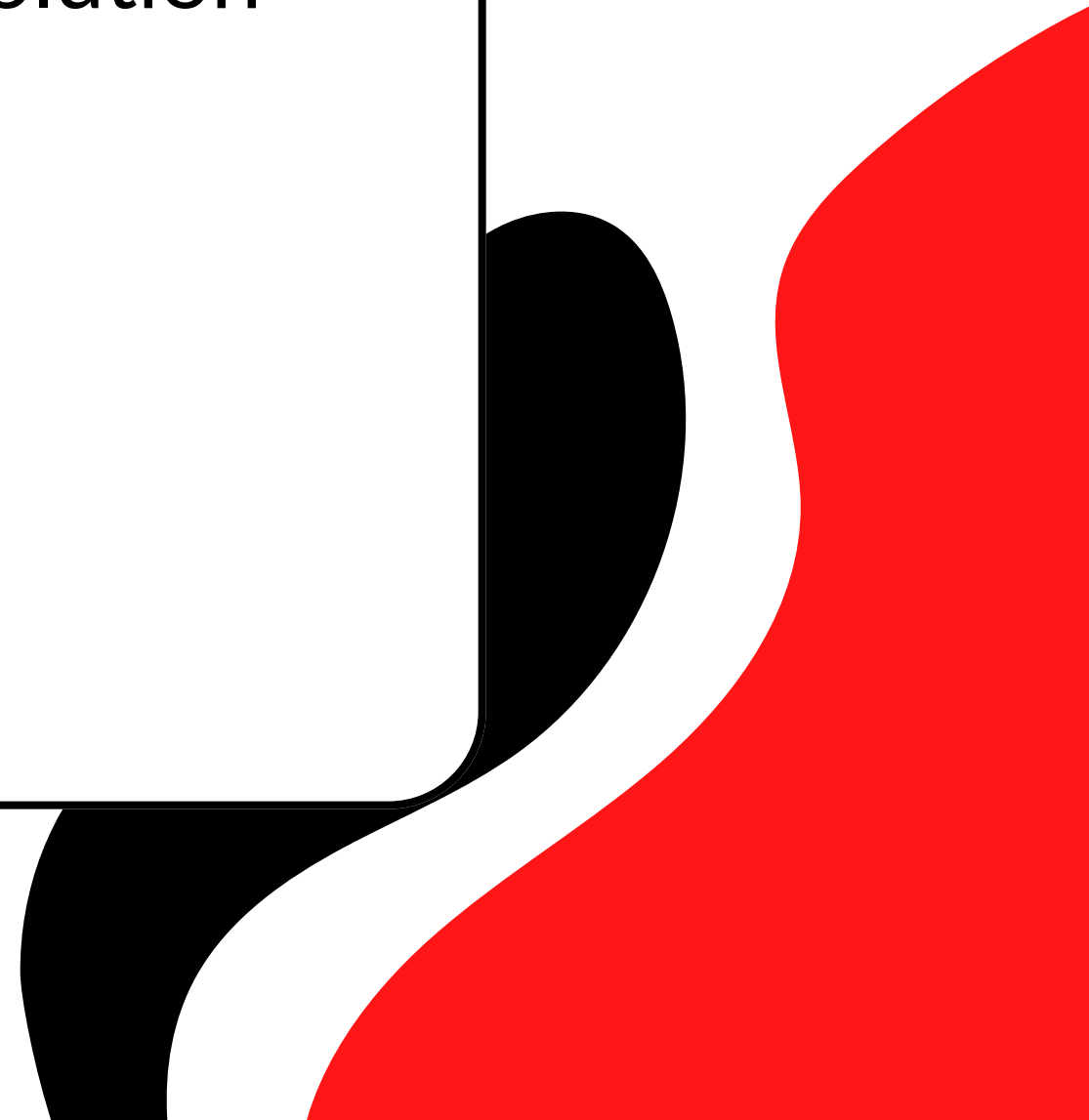
MAPPING MICROSOFT CVEs FROM UPDATE NAMES (KB)

26-02-25

<https://sidorocs.github.io>



TABLE OF CONTENT

- 
- Context
 - Some definitions
 - Problem statement
 - Toward a solution
 - References
- 

CONTEXT

Scenario :

- You are a cybersecurity engineer / a CISO
- You are supposed to handle the security of the information system of your company
- You would like to keep track on vulnerabilities that pops with time on your machines
- What can you do ?

“Couldn't you update all your machines as soon as an update is released?”



GLOSSARY

Definitions, recall ... whatever

Known Affected Software Configurations

Configuration 1 ([hide](#))

✖ cpe:2.3:o:microsoft:windows_10_1507:*:*:*:*:*:x64:*

[Show Matching CPE\(s\)](#)▼

✖ cpe:2.3:o:microsoft:windows_10_1507:*:*:*:*:*:x86:*

[Show Matching CPE\(s\)](#)▼

CVE

Public ID for a security flaw in software or hardware. It helps identify and fix vulnerabilities.

NVD

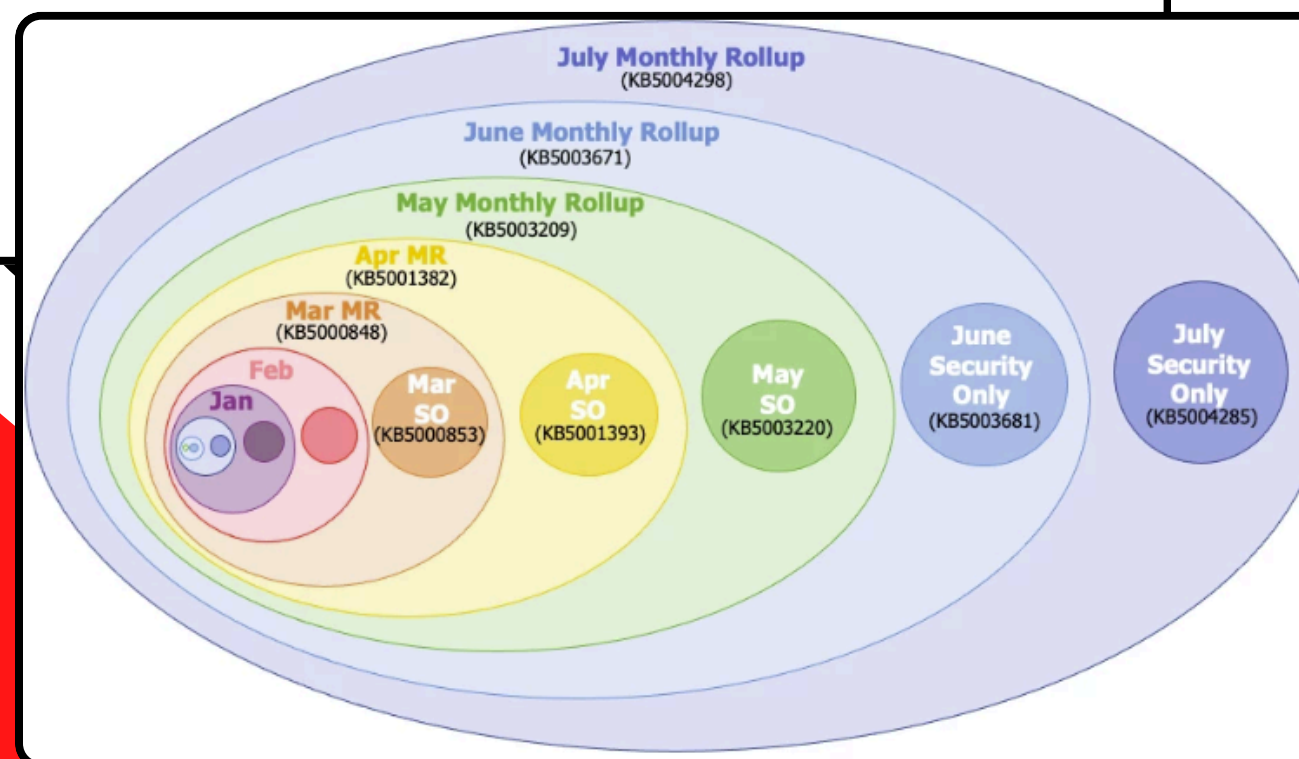
National Vulnerability Database, list of known security problems in software, managed by NIST.

CPE

System used to name and identify software, hardware, and systems. It helps to track products and vulnerabilities across different platforms.

GLOSSARY

Microsoft updates



PATCH TUESDAY

Since October 2003, Microsoft has released security updates on the second Tuesday of each month, known as Patch Tuesday

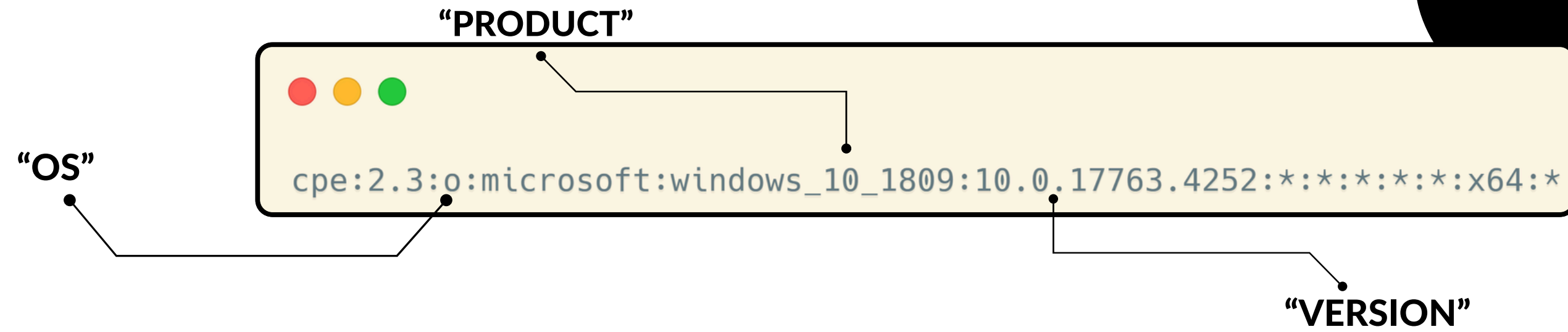
KNOWLEDGE BASIS (KB)

Microsoft Knowledge Base (KB) articles describe issues in Microsoft products. Security updates are labeled "KB" followed by a number, but since they're not sequential, tracking patch levels can be confusing.

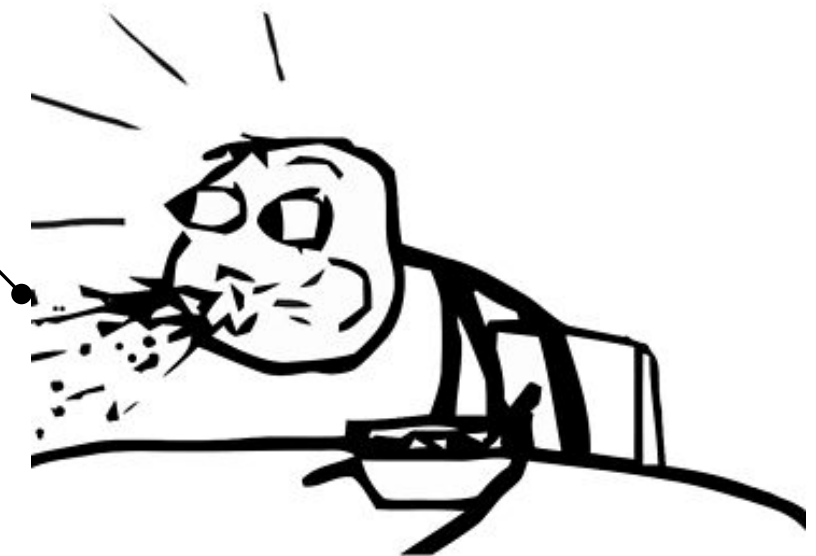
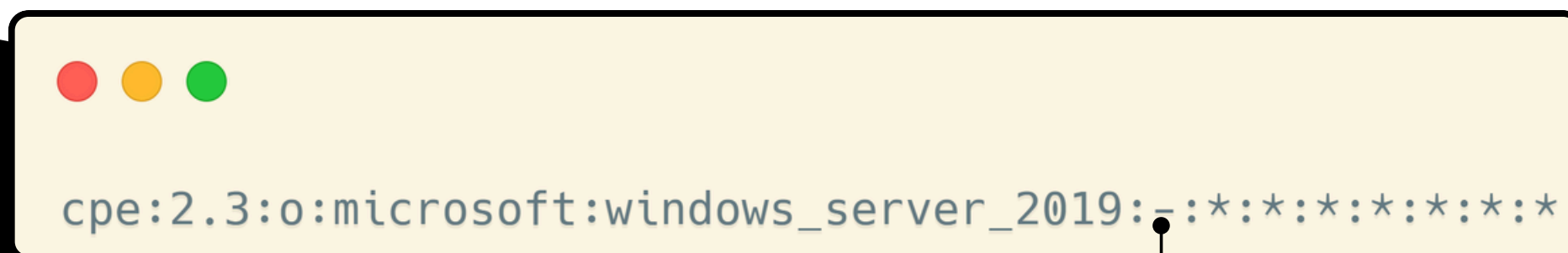
TYPE OF UPDATE

- Monthly Rollups (cumulative updates)
- Security-only Updates

“GOOD CPE”



“BAD CPE”





PROBLEM STATEMENT

We need to find a way to “determine which vulnerabilities are resolved given a list of installed patches”. In addition, we would like to automate this process !

If we rely solely on the NVD, we may encounter a large number of false positives. It's essential to apply filtering to identify relevant CVEs !



MICROSOFT SECURITY RESPONSE CENTER (MSRC)

- Provide (free) APIs to download security vulnerability reports
- One new report each month
- Following “common vulnerability reporting framework” (CVRF)
- Detailing each vulnerabilities and mitigations developed for a given month (including workarounds and patches)
- For any updates, the kb number is given with the supersedes kb number


```

{
  "document": {␣},
  "product_tree": {␣},
  "vulnerabilities": [
    {
      "cve": "CVE-2023-46281",
      "cwe": {
        "id": "CWE-942",
        "name": "Permissive Cross-domain Policy with Untrusted Domains"
      },
      "notes": [
        {
          "category": "summary",
          "text": "When accessing the UMC Web-UI from affected products,
            UMC uses an overly permissive CORS policy. This could allow an
            attacker to trick a legitimate user to trigger unwanted
            behavior.",
          "title": "Summary"
        }
      ],
      "product_status": {␣},
      "remediations": [␣],
      "scores": [␣],
      "title": "CVE-2023-46281"
    },
    {␣},
    {␣},
    {␣},
    {␣}
  ]
}

```

VULNERABILITY REPORTS

As mentionned in the previous slide, microsoft use CVRF and CSAF to publish their vulnerability report. But what is it



LINKING KB NUMBERS

Knowing the supersedes of each kb number, you can easily analyse multiple report and chaining kb. Then you will be able to keep trace of “which kb patched which vulnerability”.

KB N° XXXX

Patch : CVE-yyyy-id1, CVE-yyyy-id2....

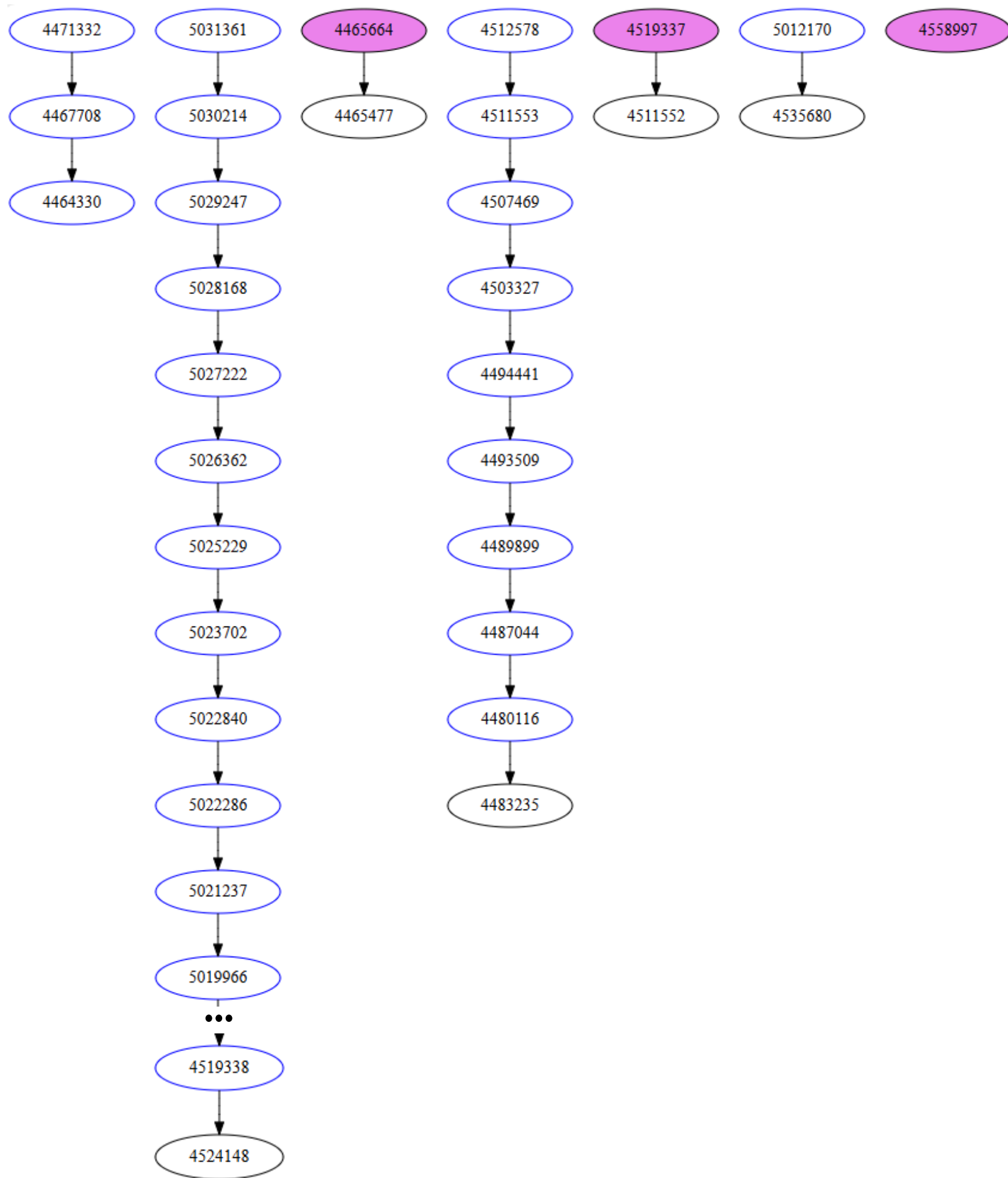
Supersedes : KB n° ZZZZ



KB N° ZZZZ

Patch : CVE-yyyy-id3, CVE-yyyy-id4....

Supersedes : -



IF U WANNA HAVE FUN...

Here's the KB dependencies graph for
windows server 2019 products...





IN PRACTICE...

The **Claroty** research team released an interesting article focusing on the same question. The difference is that they focused on another source : the Microsoft Update Catalog !

<https://claroty.com/team82/blog/from-kbs-to-cves-understanding-the-relationships-between-windows-security-updates-and-vulnerabilities>

Algorithm used in some tools :

- **Windows exploit suggerer next generation (WES-ng) :**

<https://github.com/bitsadmin/wesng>

Uses the same sources & same data processing

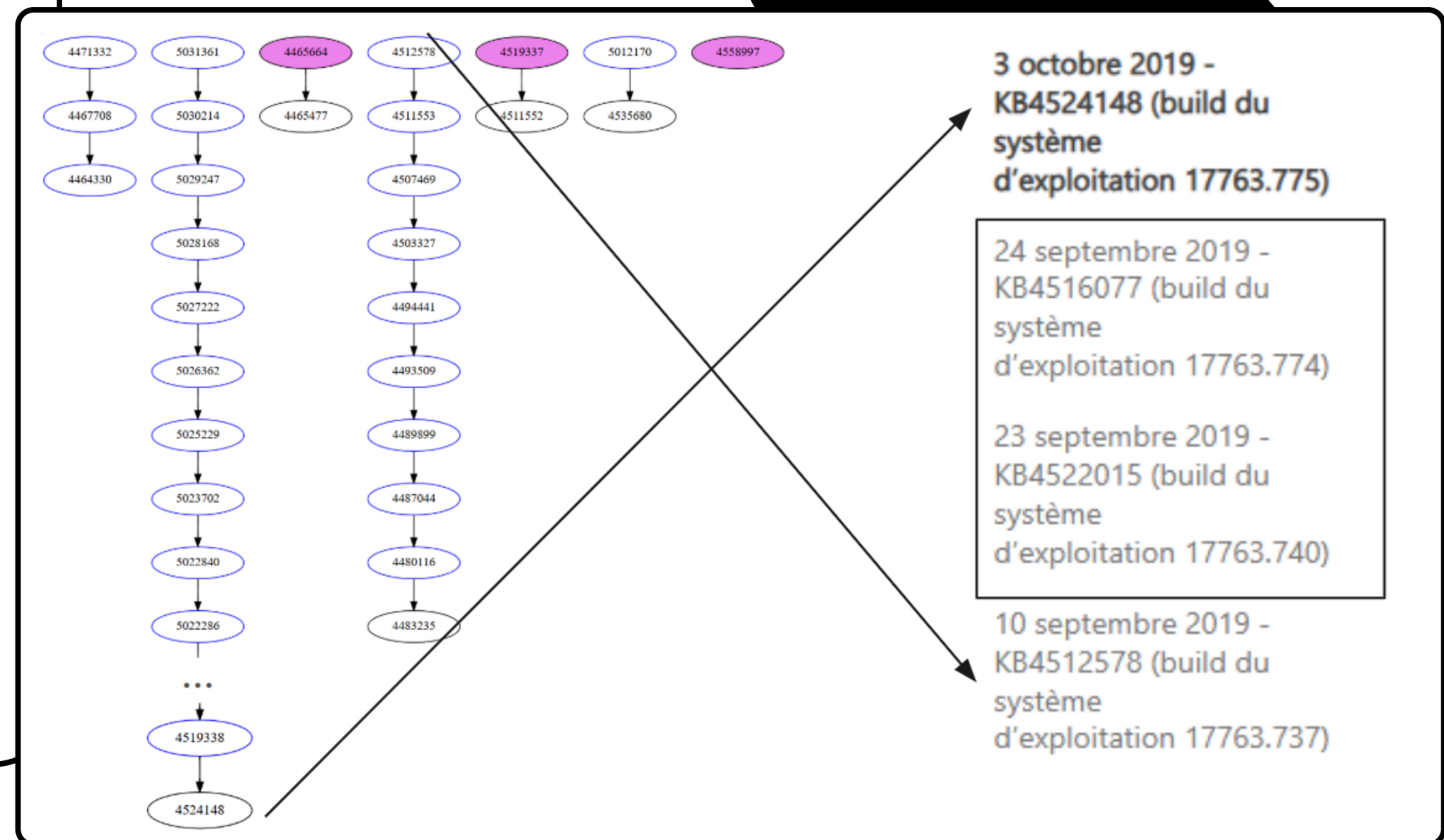
- **Wazuh :**

<https://github.com/wazuh/wazuh>

Same logic in the code but uses internal database (which is not publicly available)

STILL SOME ISSUES...

Even though the solution looks nice in theory, there is still some issues. One of them is the fact that some KB number are not referenced in the MSRC database...





STILL SOME ISSUES...

Claroty article also faces problems of holes the microsoft database. They also never mentionned about certain types of update, the cumulative security update...



To Be Continued

REFERENCES

- Claroty's article : <https://claroty.com/team82/blog/from-kbs-to-cves-understanding-the-relationships-between-windows-security-updates-and-vulnerabilities>
- OASIS, CSAF/CVRF documentation : <https://oasis-open.github.io/csaf-documentation/#>
- Microsoft update catalog : <https://www.catalog.update.microsoft.com/Home.aspx>
- API microsoft : <https://api.msrc.microsoft.com/cvrf/v3.0/swagger/v3/swagger.json>
- Me ?

THANK YOU

QUESTIONS ?

