GALEAX x cyberwatch

SecurityForum – Technical Conference - 13/02/2025

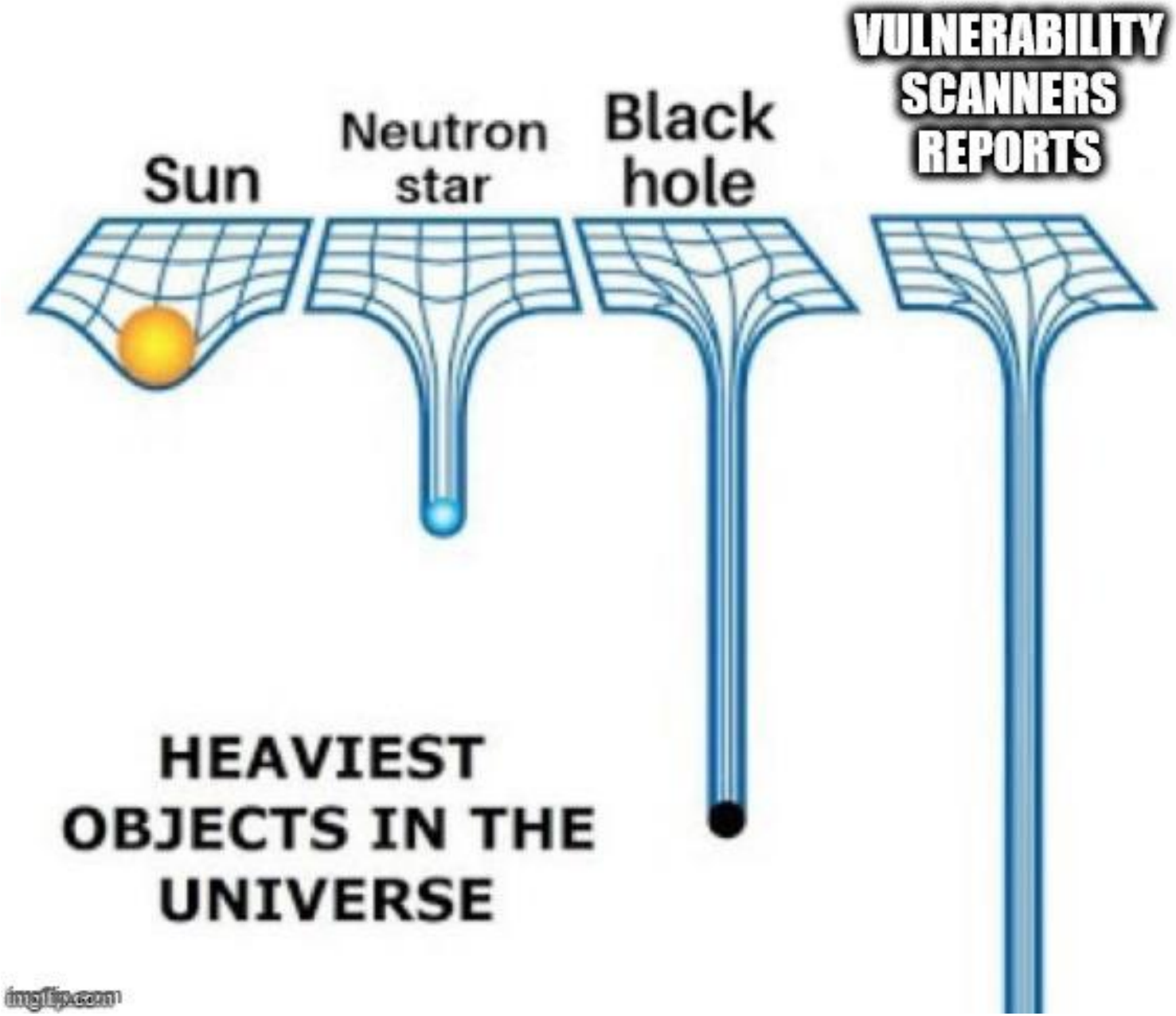
How to prioritize CVE vulnerabilities with the 3D method (CVSS-BTE + EPSS + CERT data)?

Quick intro

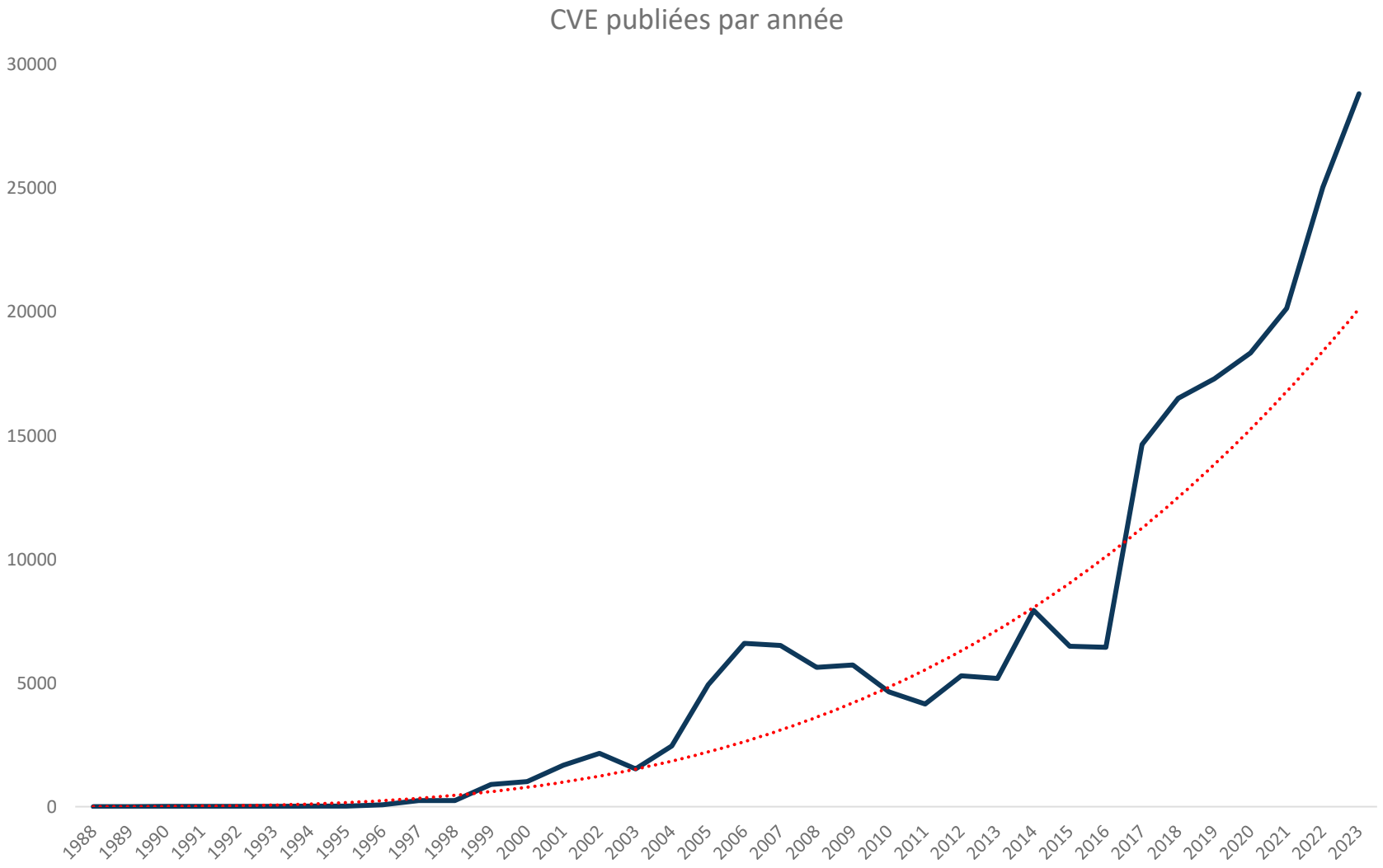
Maxime ALAY-EDDINE

French engineer
First steps in cybersecurity in 2002
Specialized in Vulnerability Management
Published multiple CVEs and contributed to bug bounty programs
Co-founder of:
- Cyberwatch (acquired by framatome in 2022)
- Galeax (Cyberwatch platinum partner) in 2023

GALEAX cyberwatch


Sun
Neutron star
Black hole
VULNERABILITY SCANNERS REPORTS
HEAVIEST OBJECTS IN THE UNIVERSE
imgflip.com

+40 000 CVE released in 2024 (+100/d!)



Vulnerability Management is a bottleneck for cybersecurity teams, but also for the NVD

NVD Program Announcement UPDATED - April, 25th 2024

NIST maintains the National Vulnerability Database (NVD), a repository of information on software and hardware flaws that can compromise computer security. This is a key piece of the nation's cybersecurity infrastructure.

There is a growing backlog of vulnerabilities submitted to the NVD and requiring analysis. This is based on a variety of factors, including an increase in software and, therefore, vulnerabilities, as well as a change in interagency support.

Currently, we are prioritizing analysis of the most significant vulnerabilities. In addition, we are working with our agency partners to bring on more support for analyzing vulnerabilities and have reassigned additional NIST staff to this task as well.

We are also looking into longer-term solutions to this challenge, including the establishment of a consortium of industry, government, and other stakeholder organizations that can collaborate on research to improve the NVD.

NIST is committed to its continued support and management of the NVD. Currently, we are focused on our immediate plans to address the CVE backlog, but plan to keep the community posted on potential plans for the consortium as they develop.

For questions and concerns, you can contact nvd@nist.gov.

Created February 13, 2024 , Updated April 25, 2024

New methods have emerged to help you prioritize your CVEs

CVSS v2 COMMON VULNERABILITY SCORING SYSTEM

CVSS V3.1 COMMON VULNERABILITY SCORING SYSTEM

CVSS V4 COMMON VULNERABILITY SCORING SYSTEM

CVSS Meta Temp Score ?

3.6

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

ANSSI

CERT-FR

EPSS Exploit Prediction Scoring System

Known Exploited Vulnerabilities Catalog

Stakeholder-Specific Vulnerability Categorization (SSVC)

AI Score ● ● ● ● 7.8

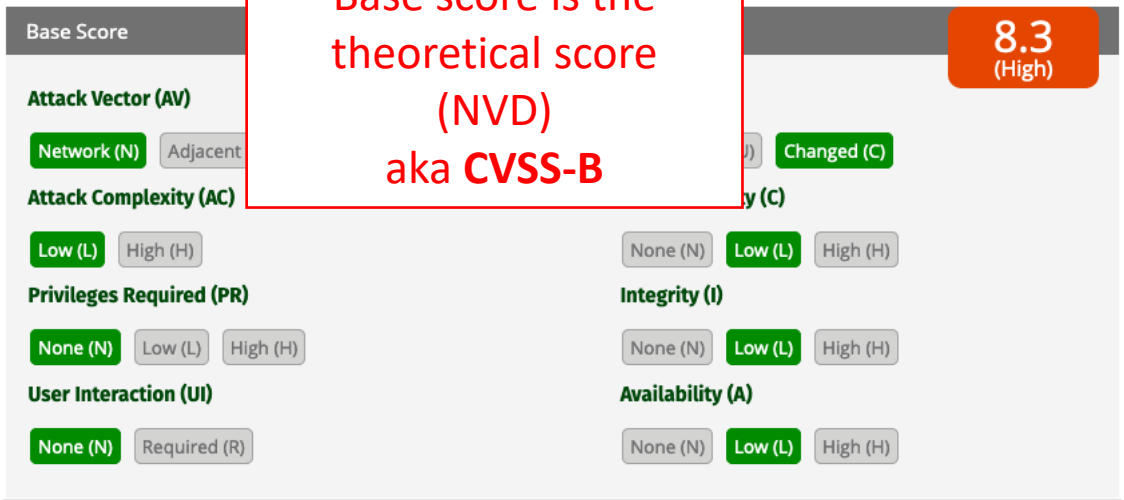
HIGH

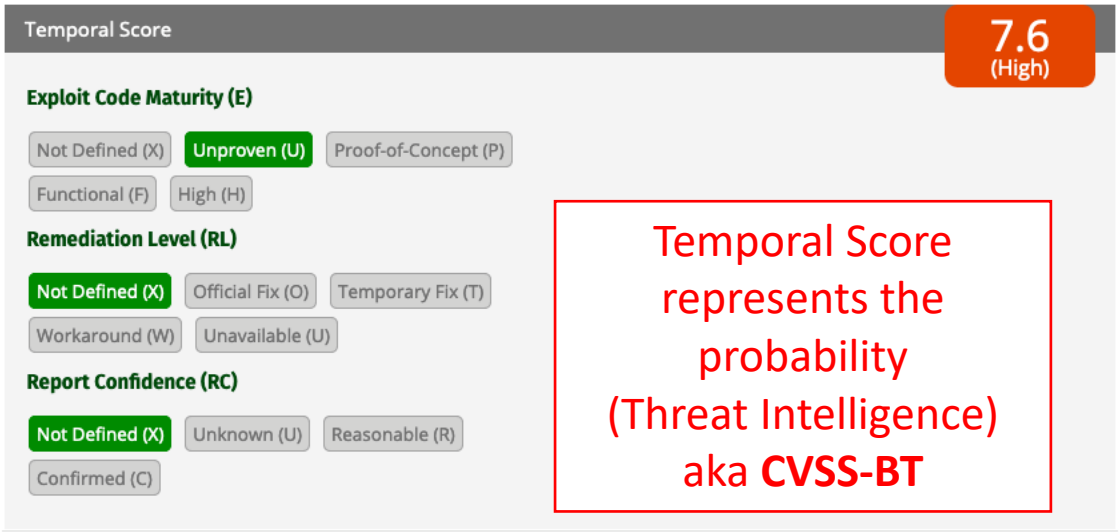
MITRE | ATT&CK®

What methods can you use to prioritize your vulnerabilities?
What are their pros and cons?
Which one should you use in 2025?

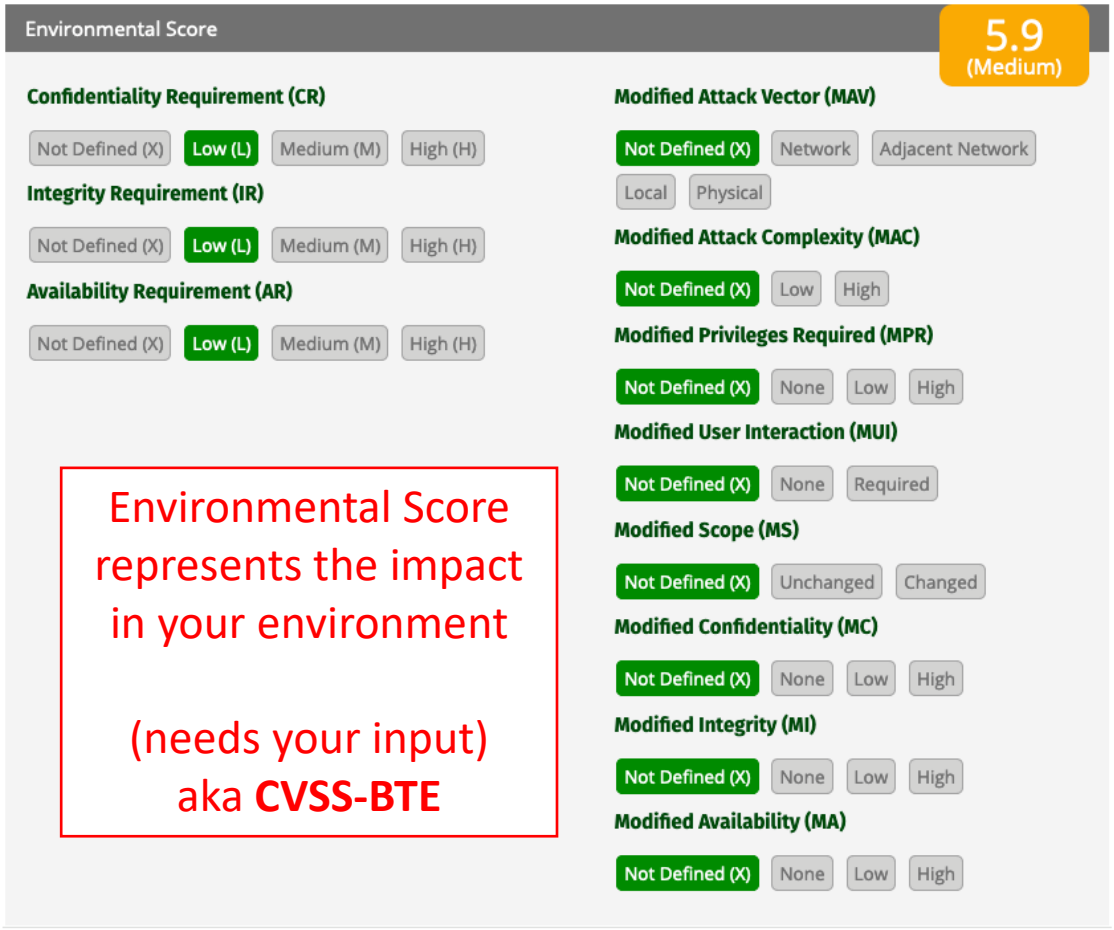
Most used scoring method today is CVSSv3.1

Base score is the theoretical score (NVD) aka **CVSS-B**





Temporal Score represents the probability (Threat Intelligence) aka **CVSS-BT**



Environmental Score represents the impact in your environment

(needs your input) aka **CVSS-BTE**

Limit #1: CVSS-B is almost always high

Mean of 2022 CVSSv3.1:

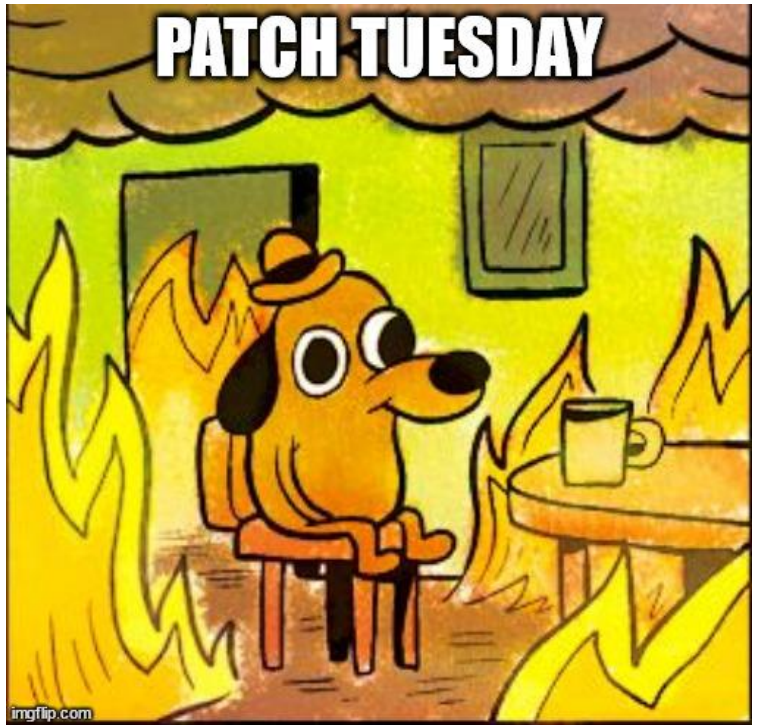
7,18 / 10

=> severity: **HIGH**

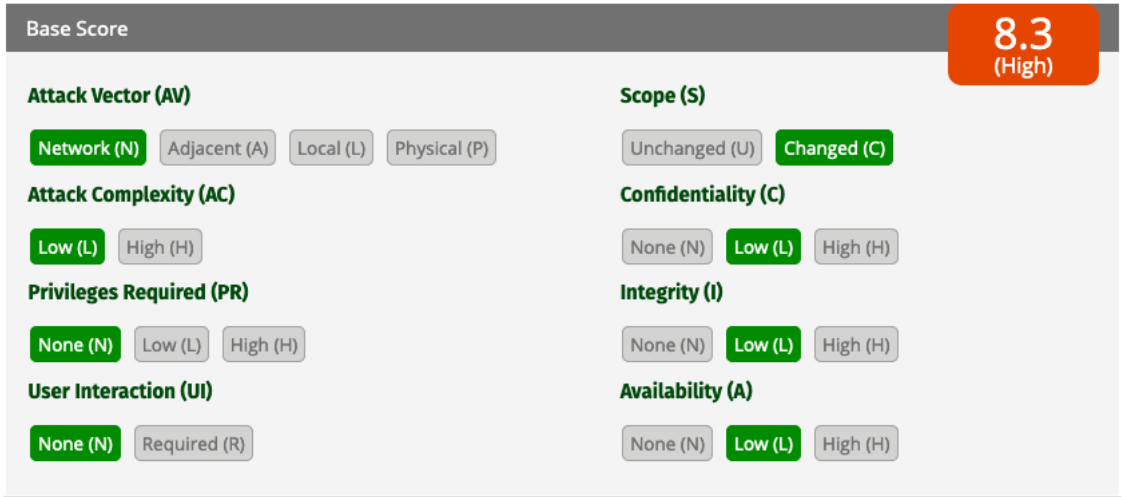
Median of 2022 CVSSv3.1:

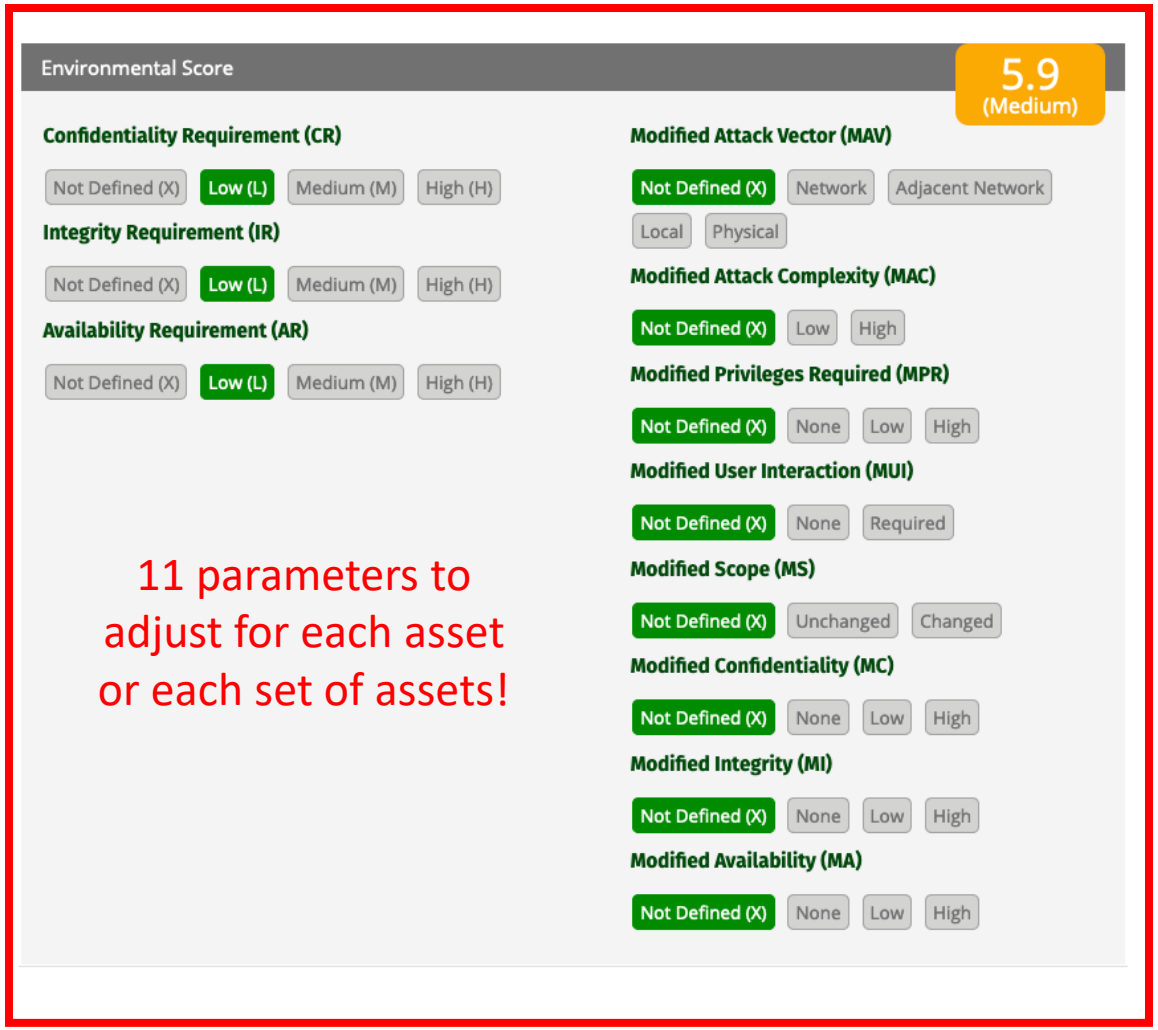
7,5 / 10

=> severity: **HIGH**

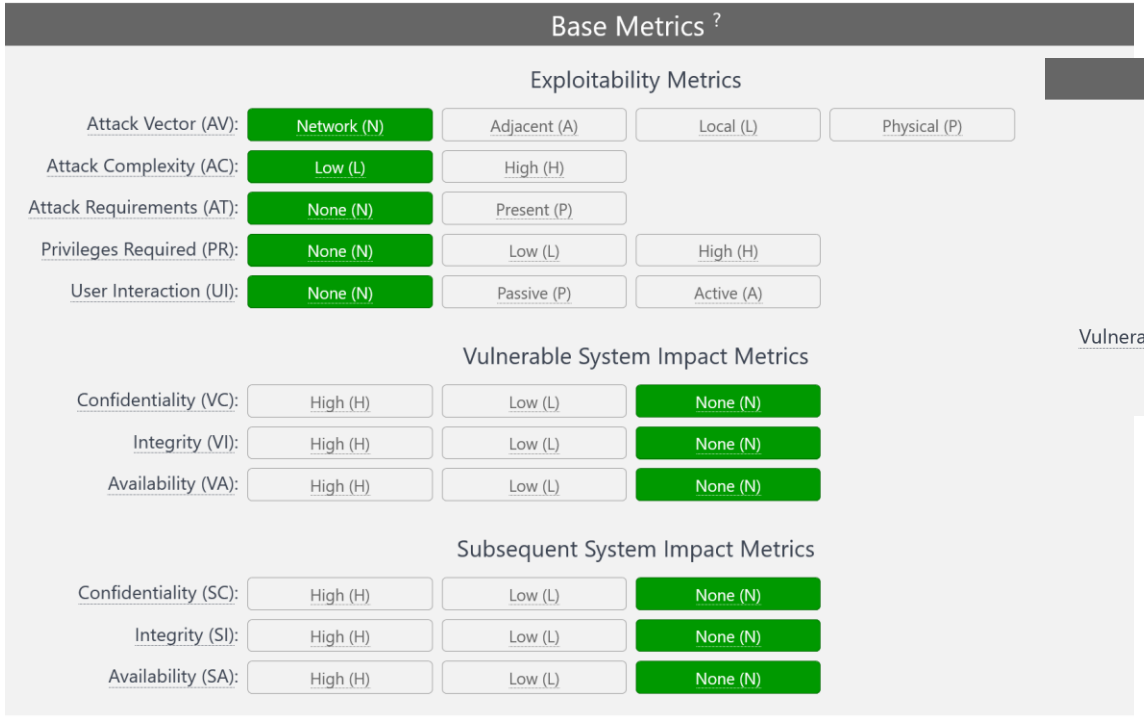


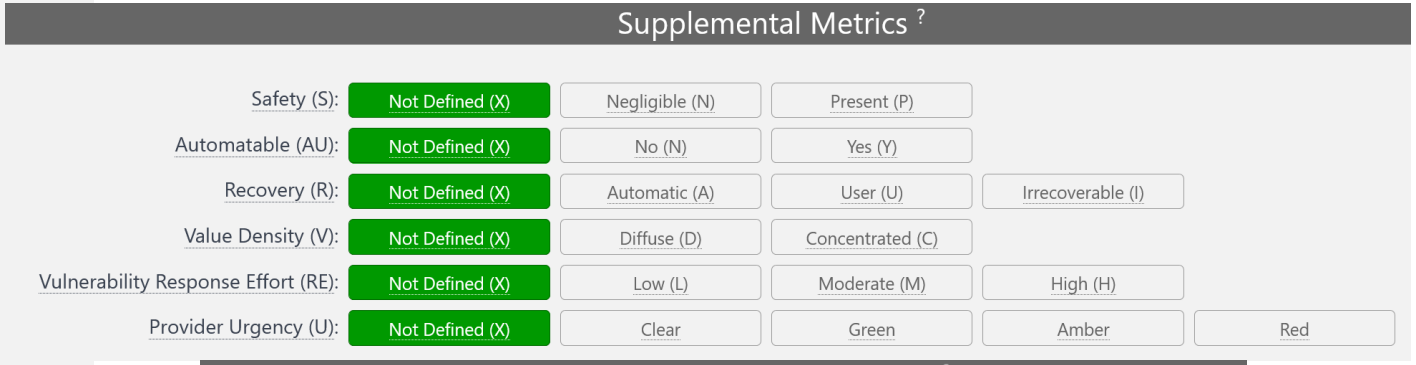
Limit #2: CVSS-BTE requires to take a lot of decisions

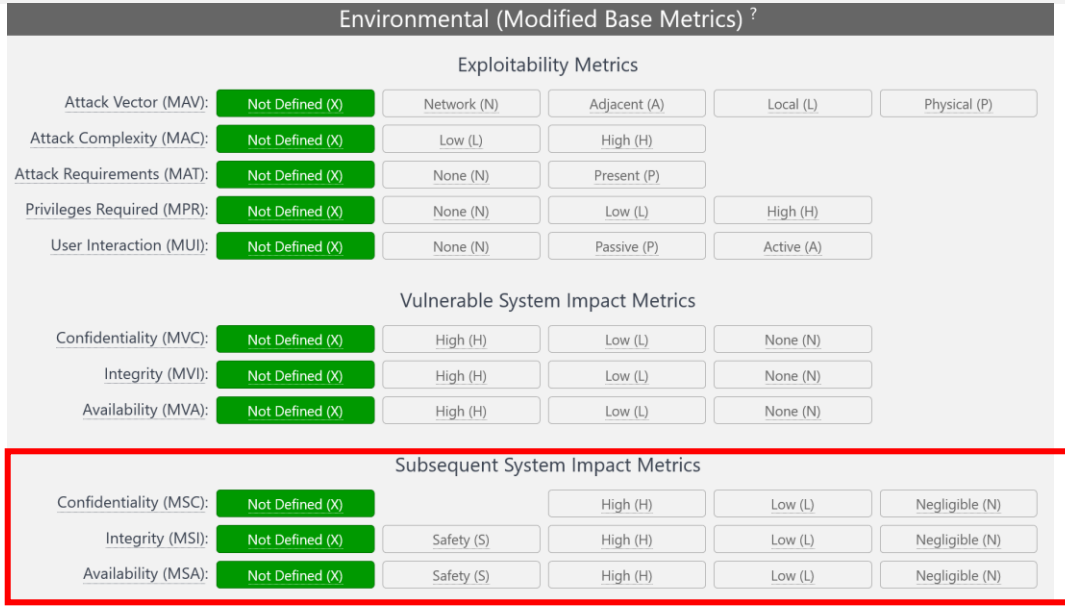


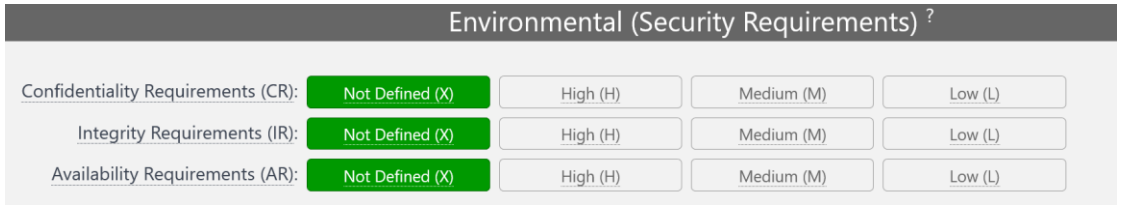


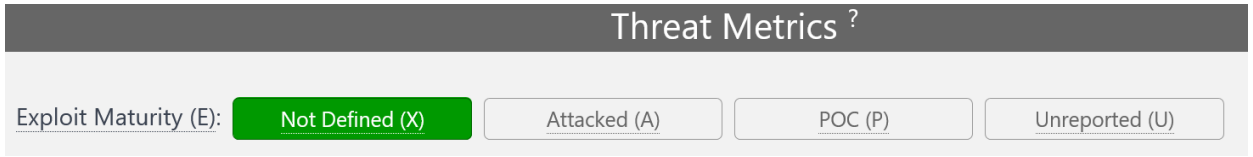
Note: CVSSv4 will not make the situation easier











New environmental parameters

A new score has been released in 2023: EPSSv3

Database with all known CVEs

1 164 variables

CVE related to Microsoft?
CVE mentioned in Metasploit?
Access Vector = Network?
Number of links mentioned by NVD?…

Database of known exploited vulnerabilites

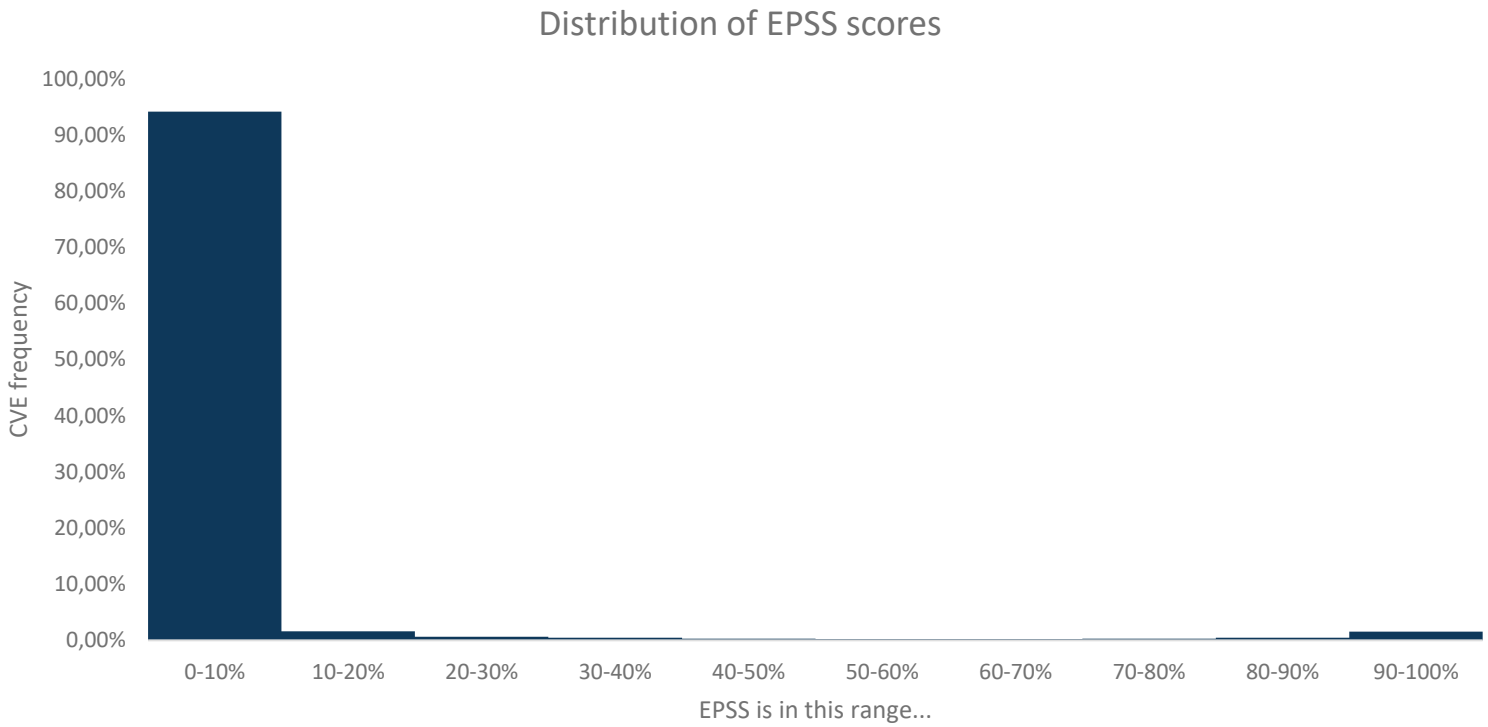
ML model that gives a **score to a CVE**, based on the **1 164 variables** of the model

cve	epss
CVE-2023-0001	0,00043
CVE-2023-0002	0,00042
CVE-2023-0003	0,001
CVE-2023-0004	0,00077
CVE-2023-0005	0,00049
CVE-2023-0006	0,00042
CVE-2023-0007	0,00045
CVE-2023-0008	0,00068
CVE-2023-0009	0,00042

EPSS can eliminate most vulnerabilities

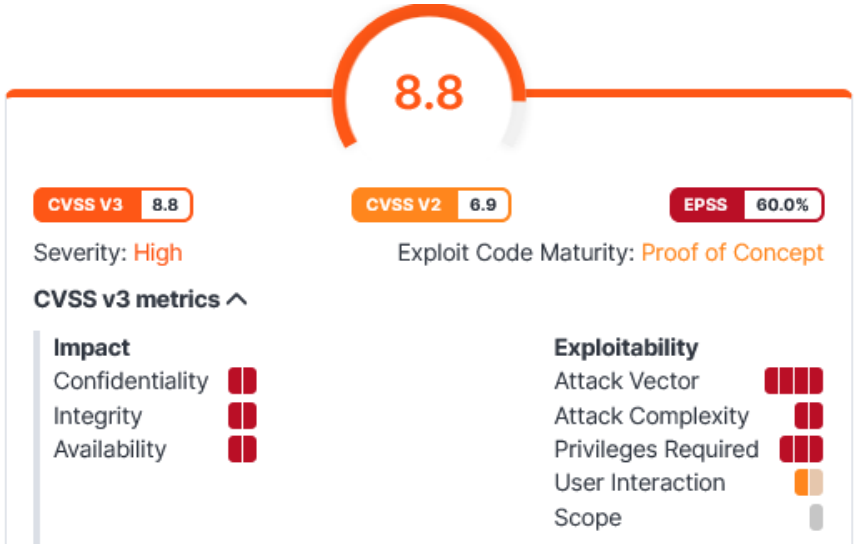
Filtering CVEs with **EPSS < 20%** will actually **remove 95%** of them!

Median: 0.143% - Mean: 3.59%



Limit #3 : EPSSv3 is not « magical »

CVE-2020-0801

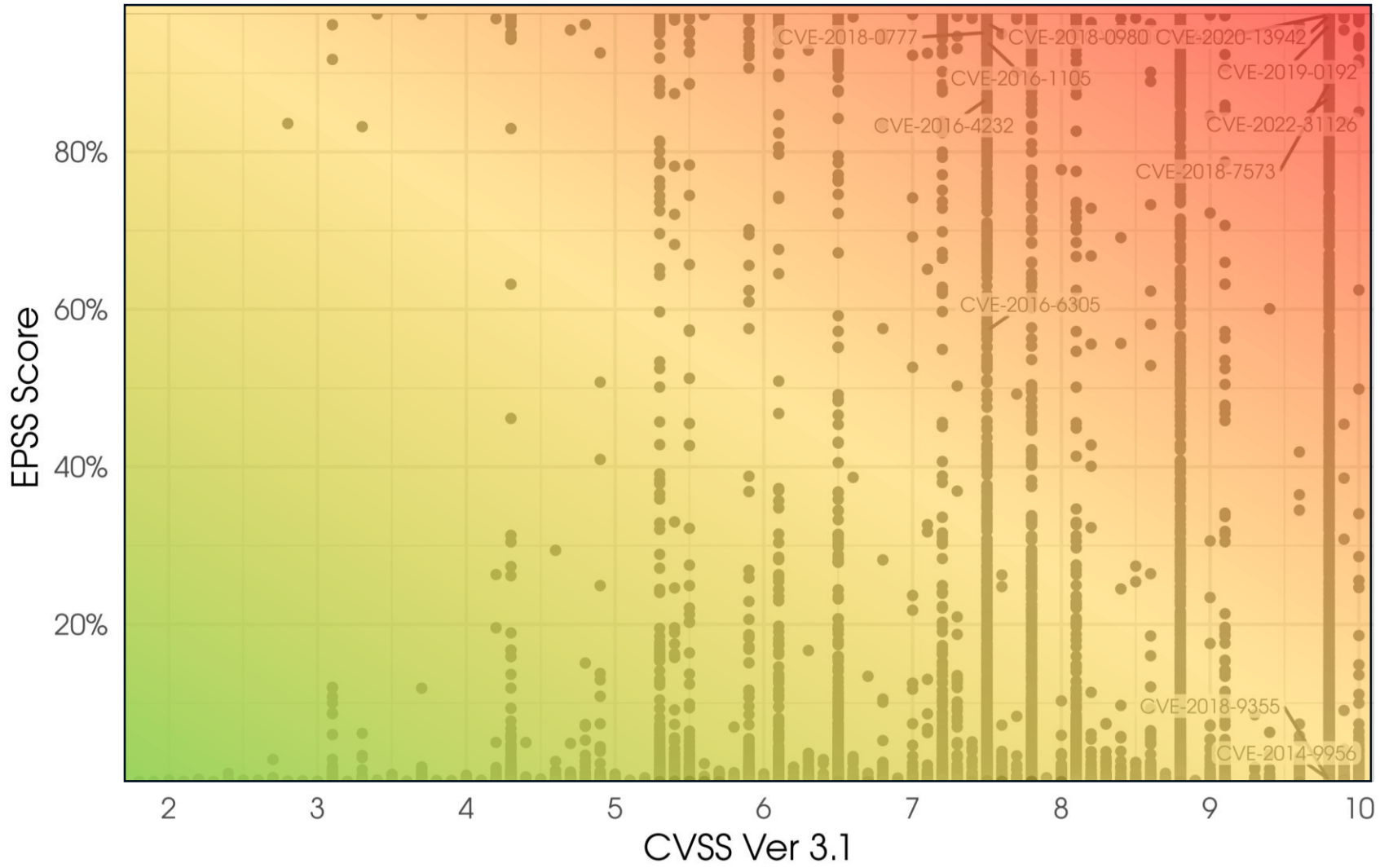


Publicly disclosed	Exploited	Exploitability assessment
No	No	Exploitation Less Likely

High EPSS, even if Microsoft says that Exploitation is Less Likely

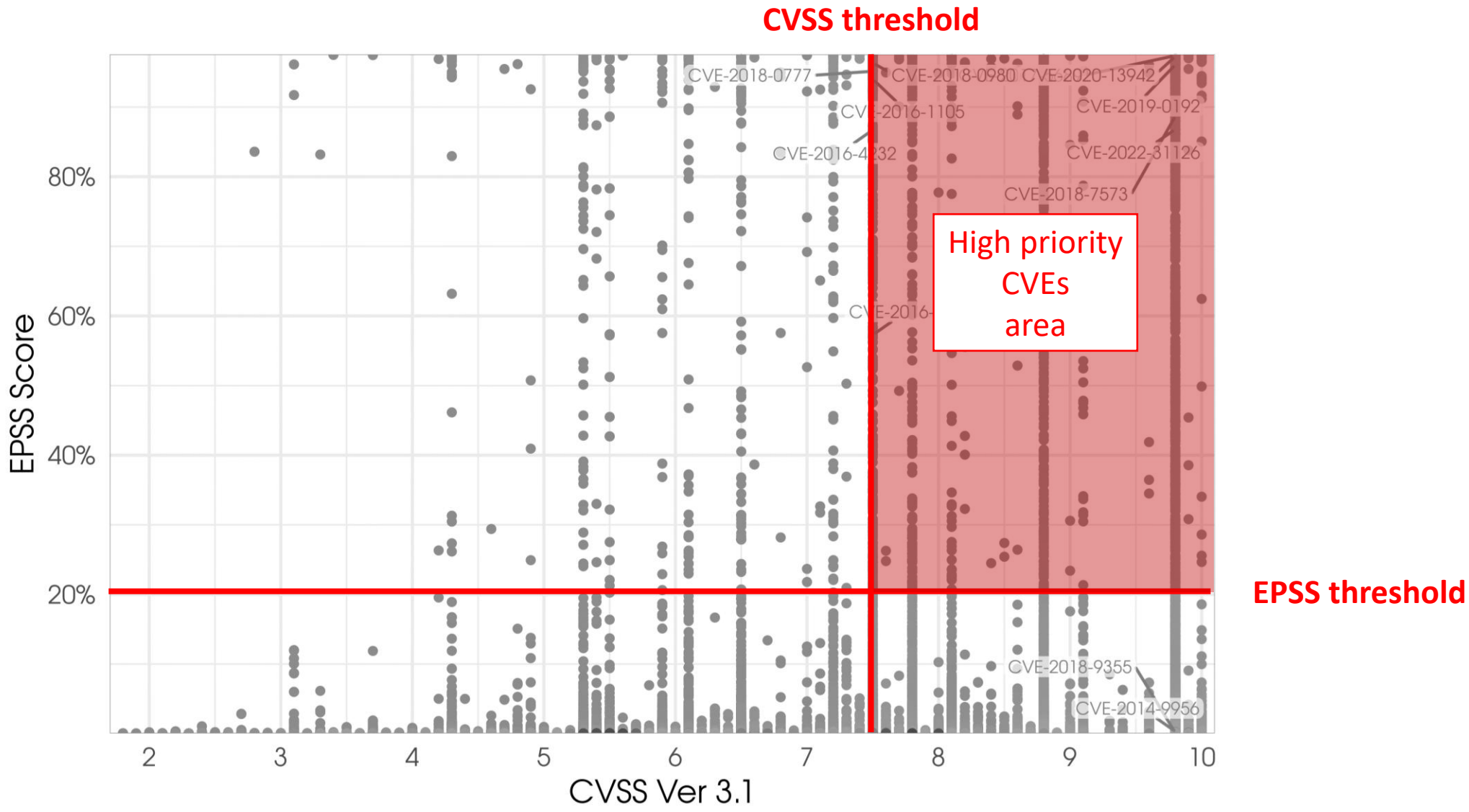
Root cause: EPSS is very influenced by the vendor of the vulnerable technology
(Microsoft => very high EPSS)

You can then plot CVEs with both their CVSS and EPSS scores



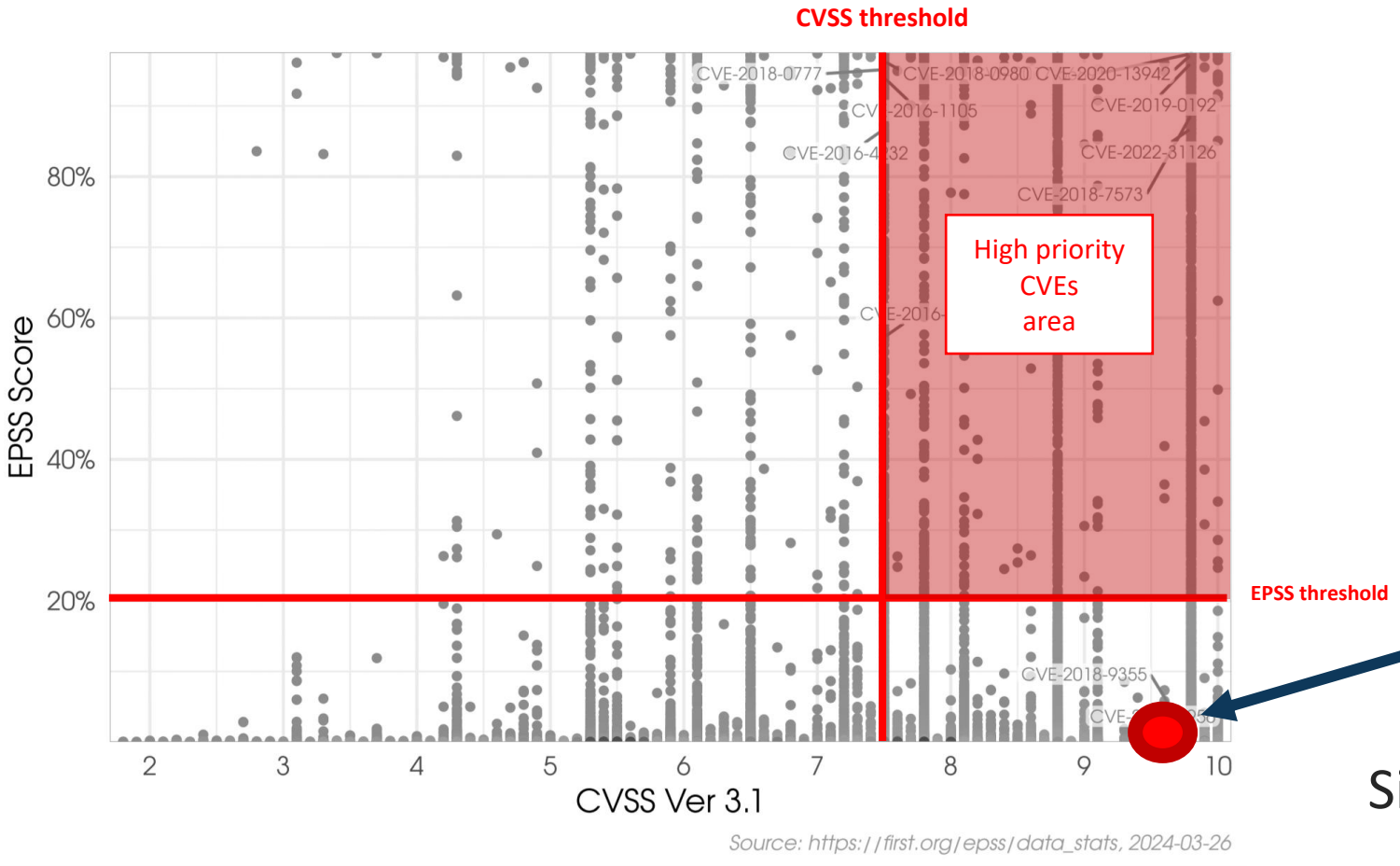
Source: https://first.org/epss/data_stats, 2024-03-26

Proposal: combine CVSS & EPSS to better sort your CVEs



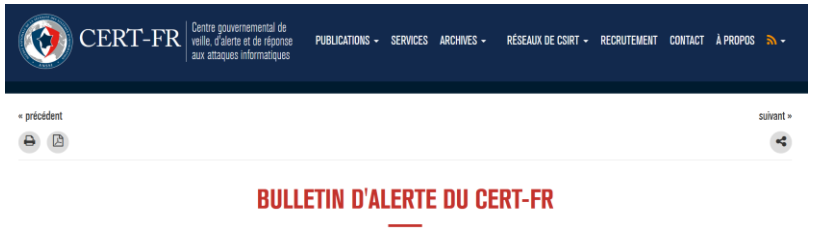
Source: https://first.org/epss/data_stats, 2024-03-26

Limit#4a: when CVEs are cherry-picked by authorities



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Known Exploited Vulnerabilities Catalog



Example:

CVE-2024-40766 (SonicWall)

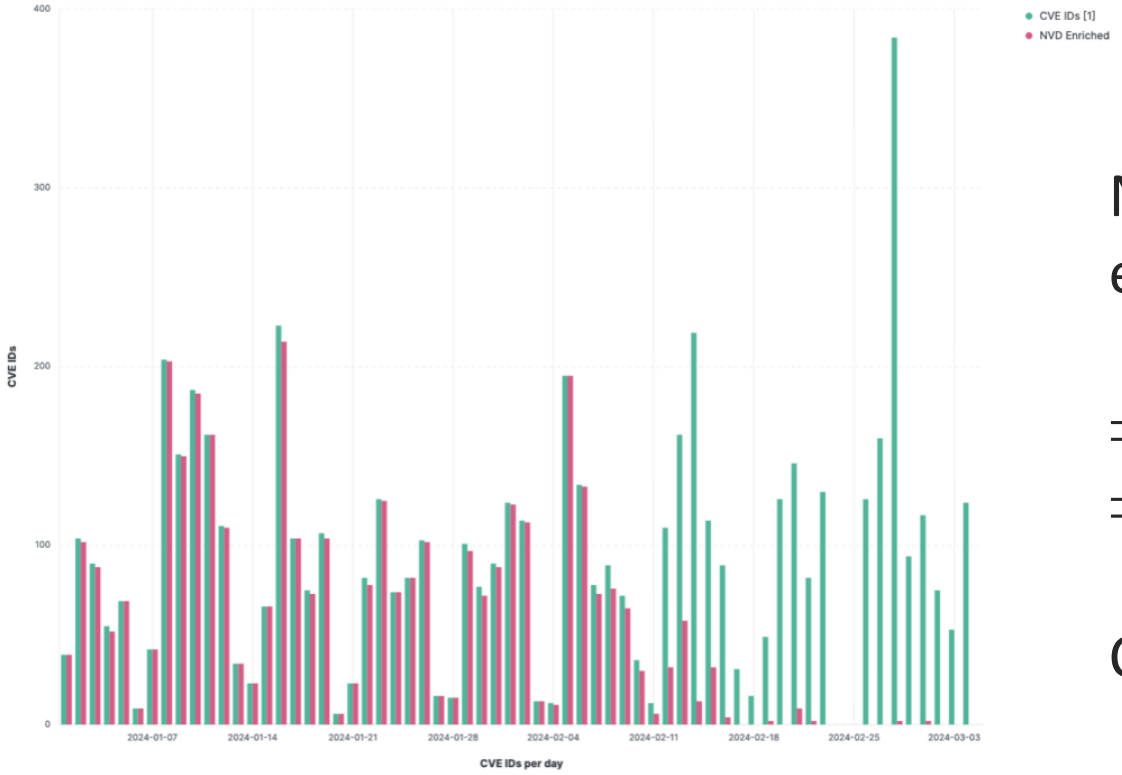
CVSS 9.8

EPSS 0.82%

Signaled by CISA KEV and CERT-FR ALE

Missed by the CVSS+EPSS method

Limit#4b: when CVEs have no official CVSS



NVD was very slow to produce new CVSS evaluations between February and June 2024

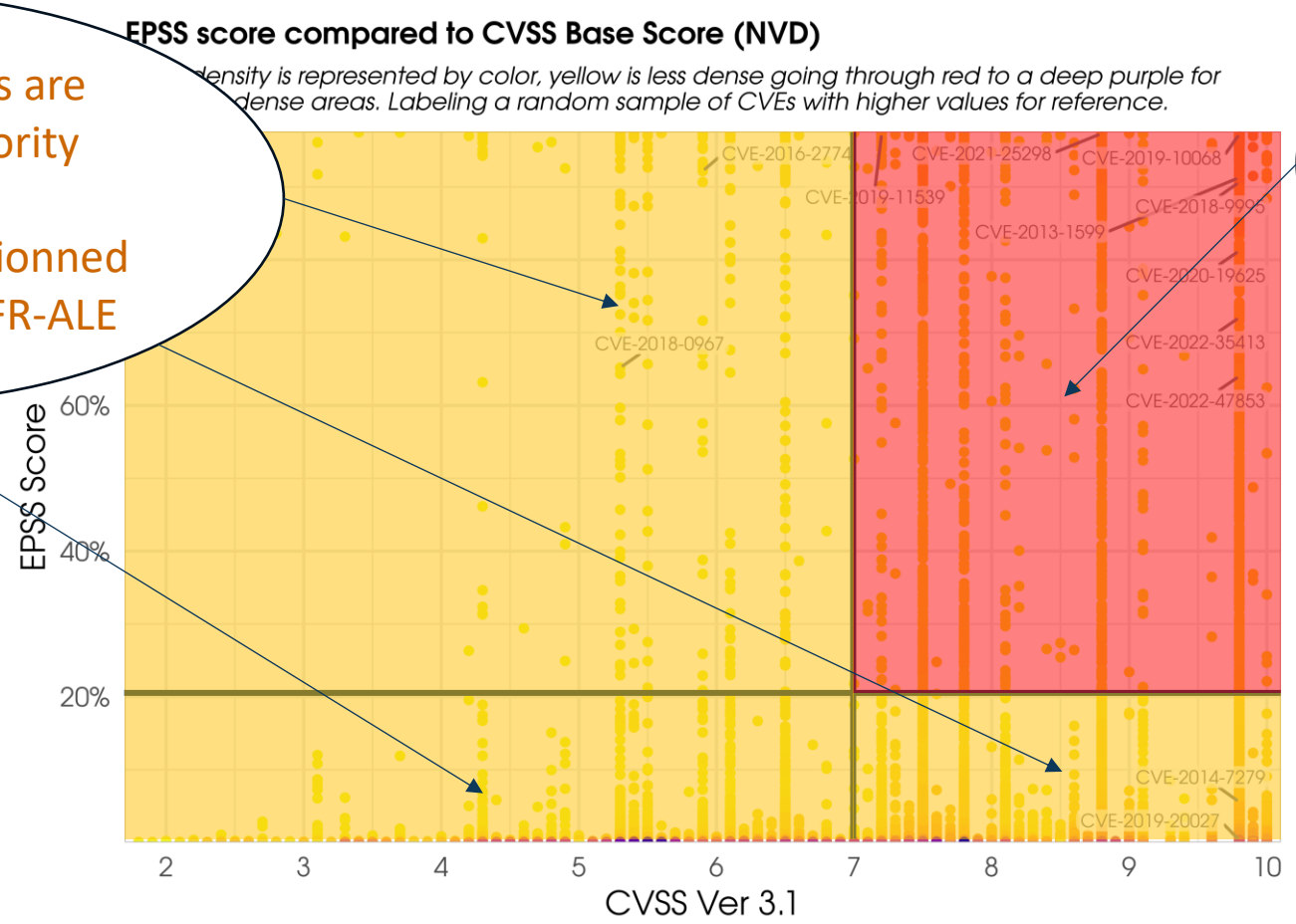
⇒ No CVSS-B, thus no CVSS-BTE…
⇒ No EPSS as well! (EPSS relies on CVSS data)

Can not plot these CVEs on the CVSS/EPSS graph!

Solution: combine CVSS + EPSS + Authorities bulletins

3D Prioritization = combination of 3 parameters CVSS / EPSS / Authorities alerts

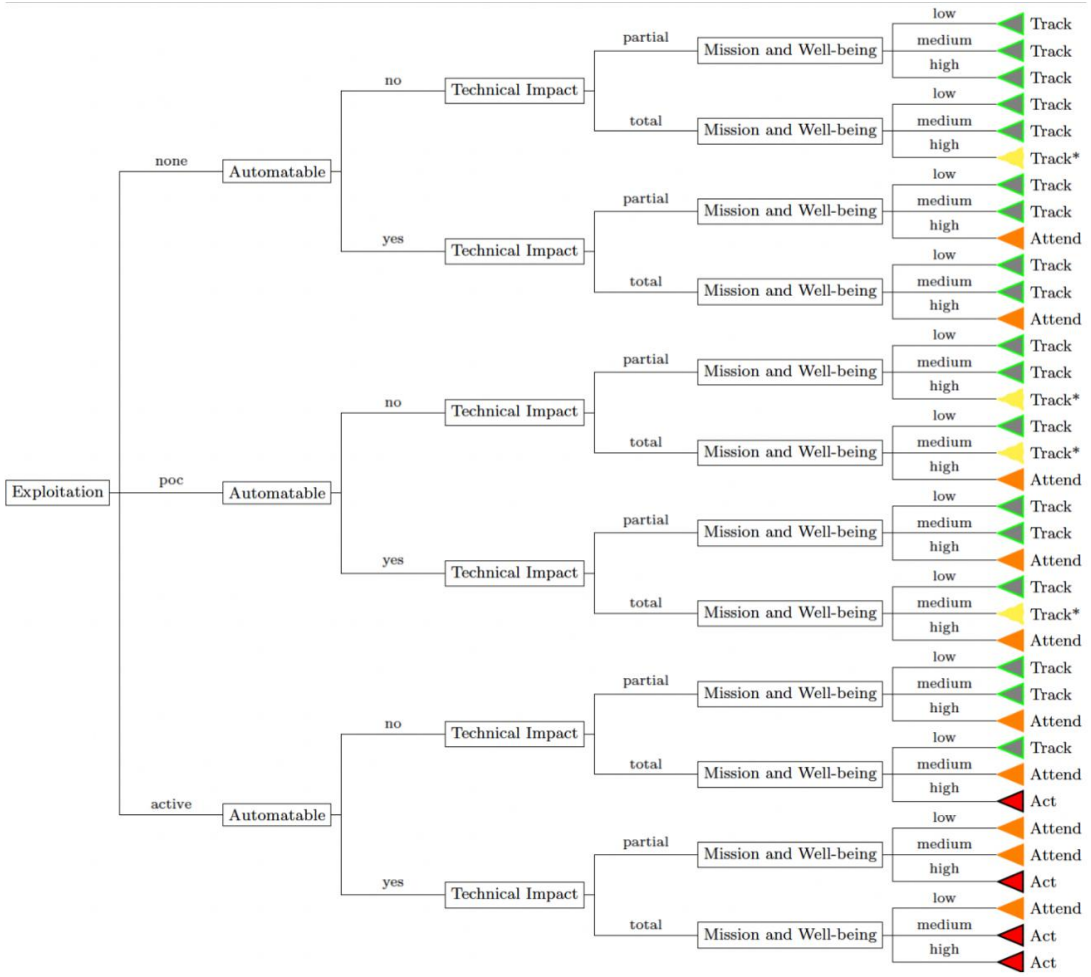
In these areas, CVEs are marked as high priority if and only if they have been mentionned by CISA KEV or CERTFR-ALE



CVE here have high priority (both CVSS & EPSS thresholds have been reached)

Remark #1: what about SSVC?

Stakeholder-Specific Vulnerability Categorization (SSVC)



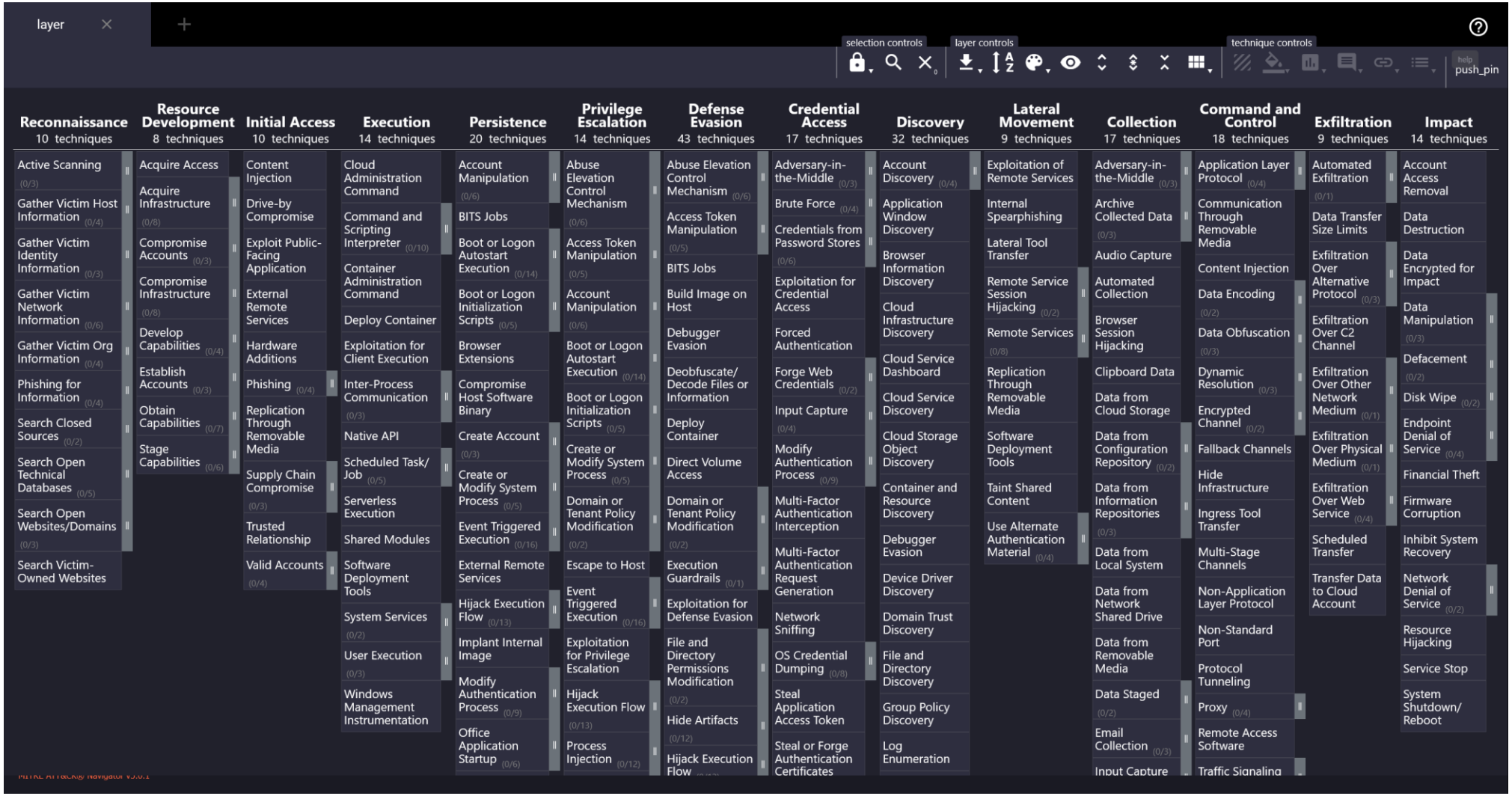
36 possible outcomes,
4 only mean « Fix this now » (Act)

Values « Exploitation, Automatable, Technical Impact » are provided by the Vulnrichment project by CISA : https://github.com/cisagov/vulnrichment/tree/develop

⇒ You only have to fill « Mission and Well-being »

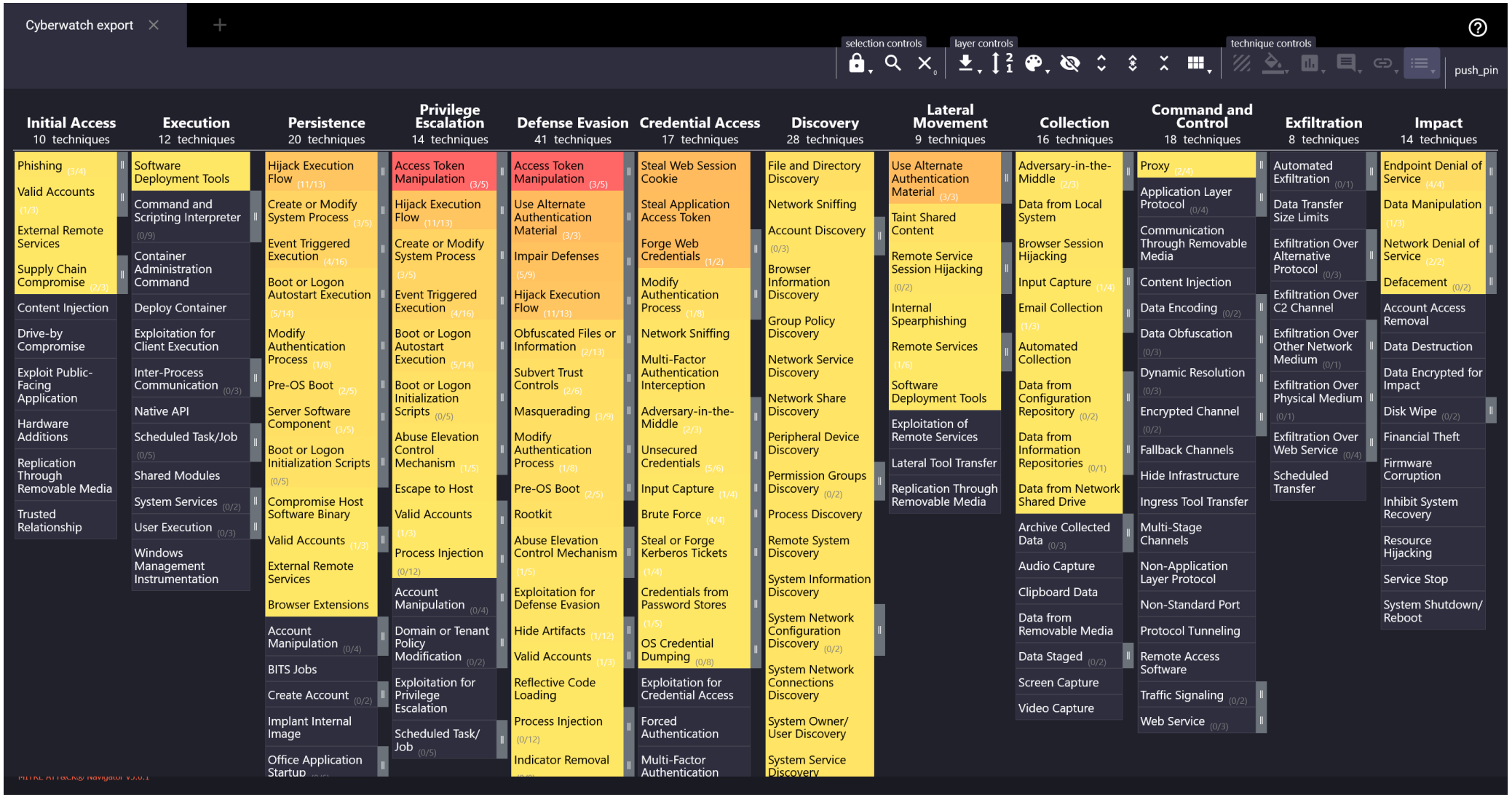
This method often leads to « Do nothing now ».
This approach is mostly used in the OT world, where deploying a patch can be very costly.

Remark #2: what about MITRE ATT&CK ?



Attack path

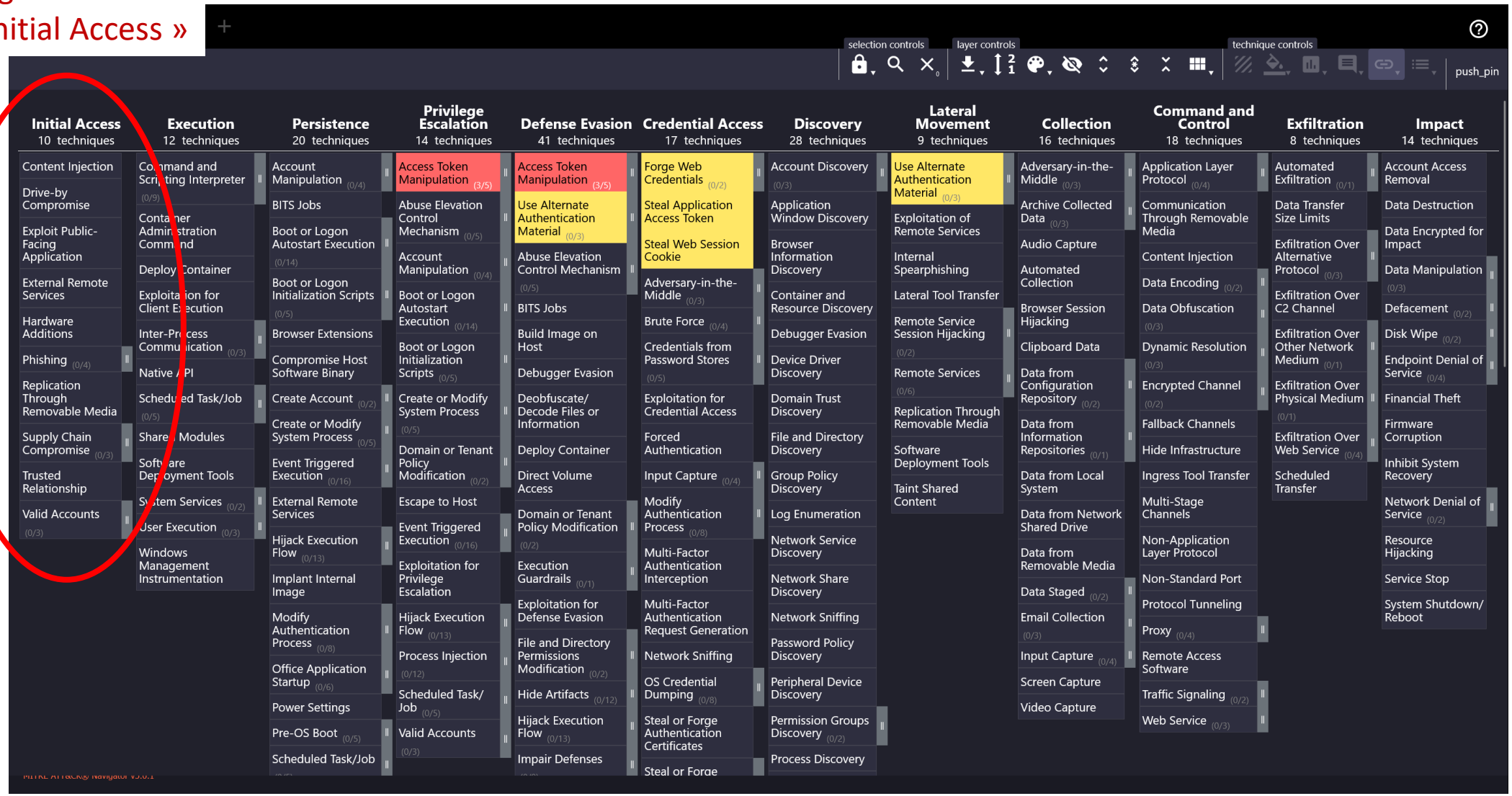
Projecting CVE (CVE -> CWE -> CAPEC -> TTPs)

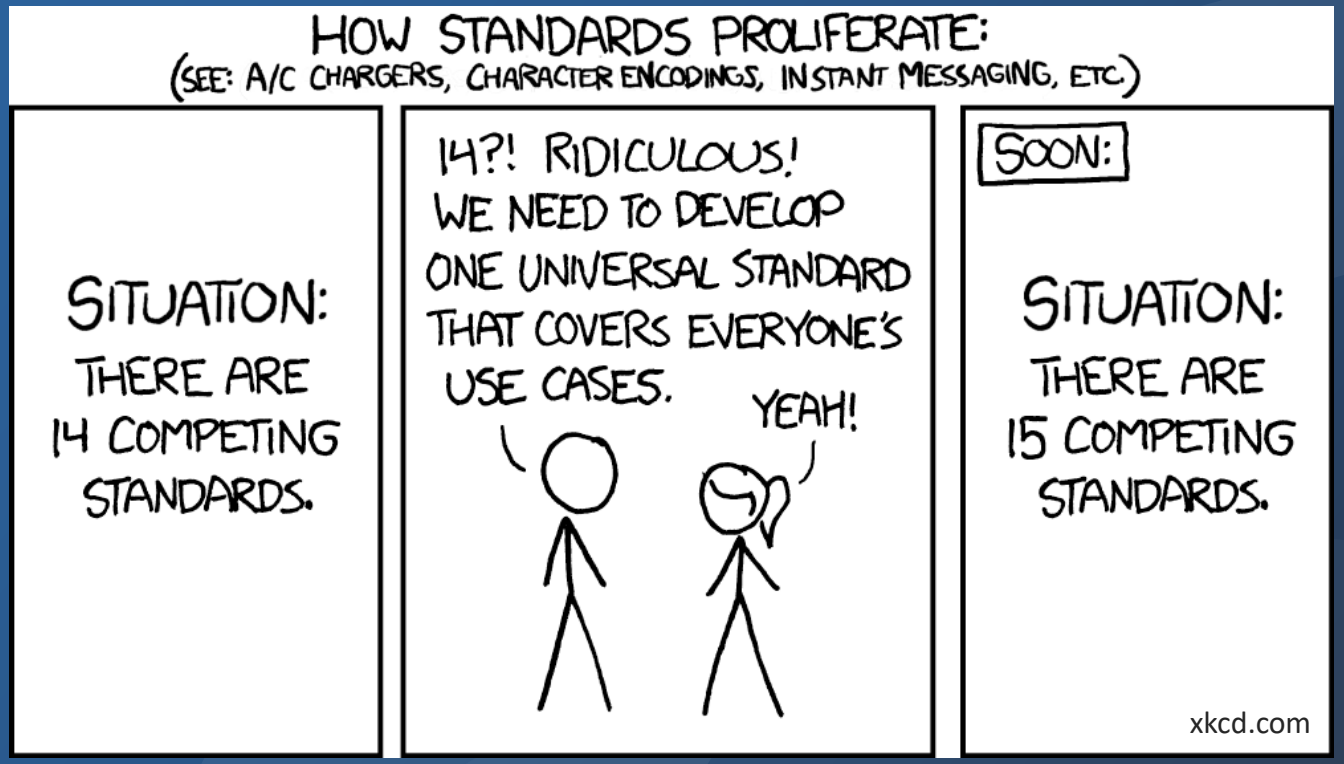


Classical approach: target the earliest steps of an attack

This method can also miss some CVEs:
Example with CVE-2024-21762 (RCE on Fortinet, widely used to start an attack)

Nothing on the first step « Initial Access »





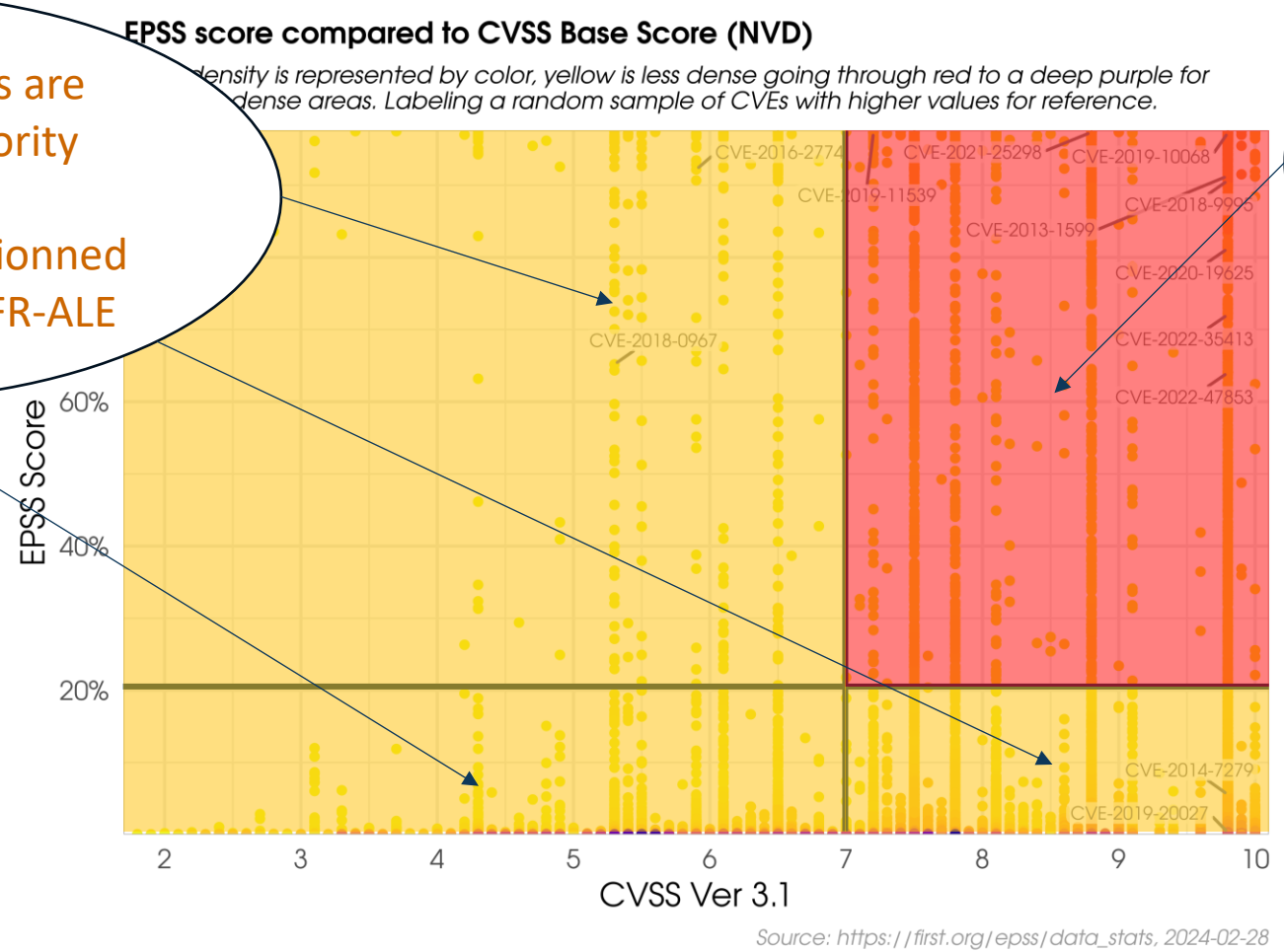
Pre-conclusion:

There is no « one fits all » magical method

Combine multiple methods and use their strengths

The pragmatic approach: « 3D Prioritization » CVSS+EPSS+Authorities data

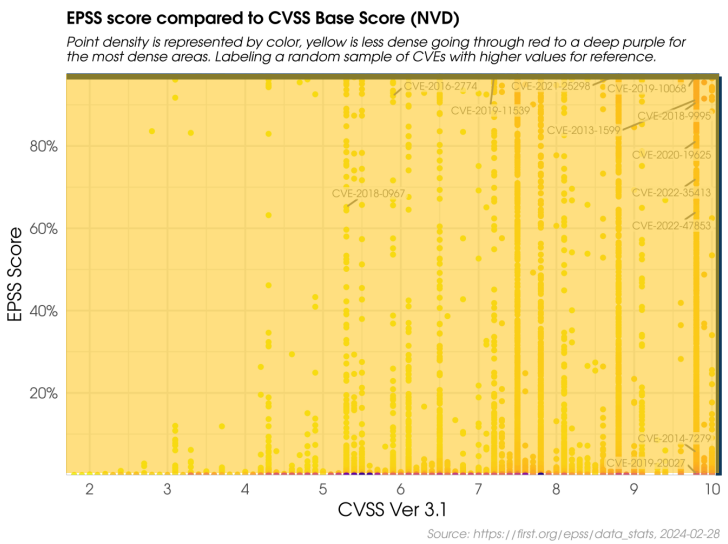
In these areas, CVEs are marked as high priority if and only if they have been mentionned by CISA KEV or CERTFR-ALE



CVE here have high priority (both CVSS & EPSS thresholds have been reached)

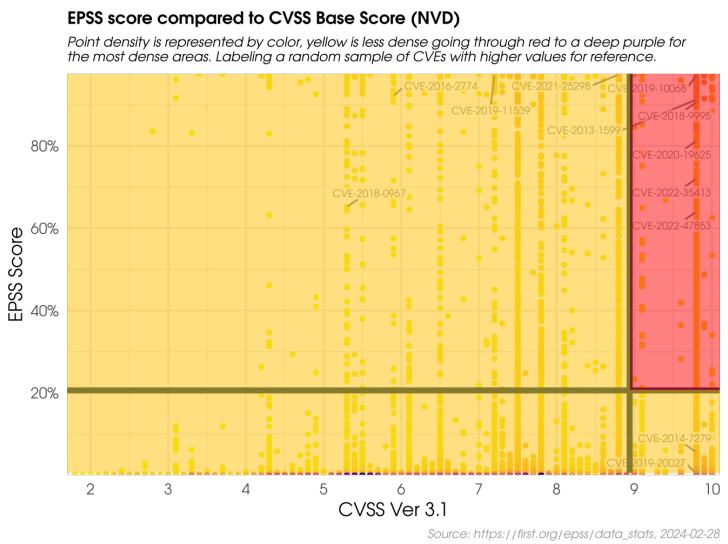
Our recommendation:
make the thresholds fit your environments

Non critical assets



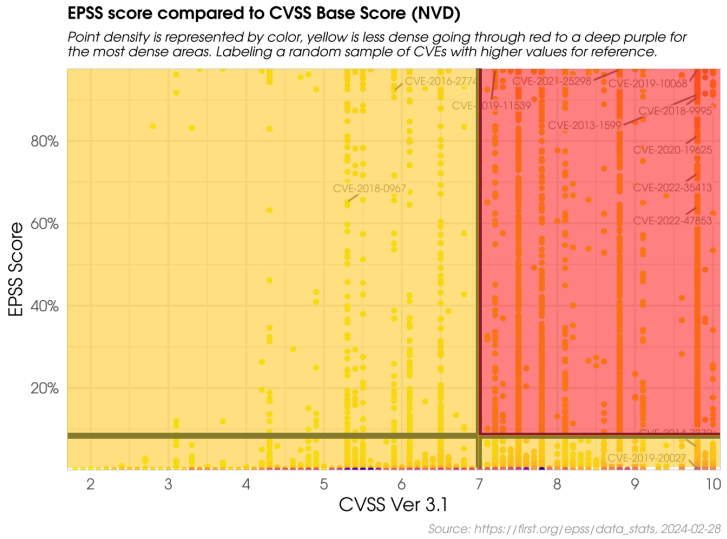
CVSS > 10
EPSS > 100%
+ CERT-FR ALE / CISA KEV

Other assets



CVSS > 9
EPSS > 20%
+ CERT-FR ALE / CISA KEV

Critical assets



CVSS > 7
EPSS > 10%
+ CERT-FR ALE / CISA KEV

Here, CVEs will be marked as high priority only if they are mentioned by authorities

This 3D Prioritization method can be fully automated…

```
maxime@CBW-DIR-MAE:~$ curl https://services.nvd.nist.gov/rest/json/cves/2.0?cveId=CVE-2019-1010218 | jq .vulnerabilities[0].cve.metrics.cvssMetricV31
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2626  100  2626    0     0   1006      0  0:00:02  0:00:02 --:--:--  1006
[
  {
    "source": "nvd@nist.gov",
    "type": "Primary",
    "cvssData": {
      "version": "3.1",
      "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
      "attackVector": "NETWORK",
      "attackComplexity": "LOW",
      "privilegesRequired": "NONE",
      "userInteraction": "NONE",
      "scope": "UNCHANGED",
      "confidentialityImpact": "NONE",
      "integrityImpact": "NONE",
      "availabilityImpact": "HIGH",
      "baseScore": 7.5,
      "baseSeverity": "HIGH"
    },
    "exploitabilityScore": 3.9,
    "impactScore": 3.6
  }
]
```

API services.nvd.nist.gov
to get the CVSS-B and build the CVSS-BTE

```
maxime@CBW-DIR-MAE:~$ curl https://api.first.org/data/v1/epss?cve=CVE-2019-1010218 | jq .data[0].epss
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   205  100   205    0     0   1090      0 --:--:-- --:--:-- --:--:--  1084
"0.001090000"
```

API api.first.org
to get the EPSS

```
maxime@CBW-DIR-MAE:~$ curl https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json | grep -c CVE-2019-1010-218
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  737k    0  737k    0     0  9965k      0 --:--:-- --:--:-- --:--:-- 9965k
0
```

JSON of the CISA to check if a CVE is mentioned (for ANSSI, use RSS feeds)

…and is already available in Cyberwatch Vulnerability Manager ☺

...and can be implemented in Excel / PowerBI / Google Spreadsheet

CVE Code	CVSS-B score	EPSS score	Mentioned by CISA KEV	Mentioned by CERT-FR ALE	DECISION
CVE-2019-1010218	7,5	0,00109	No	No	Wait
CVE-2023-7028	9,8	0,95758	Yes	Yes	Fix
CVE-2024-29988	8,8	0,00298	Yes	No	Wait
CVE-2023-38408	9,8	0,05823	No	No	Wait
CVE-2021-44228	10	0,96763	Yes	Yes	Fix
CVE-2024-6387	8,1	0,0039	No	Yes	Fix
CVE-2023-48777	9,9	0,00054	No	No	Wait
CVE-2017-0144	8,8	0,96301	Yes	No	Fix

CVSS-B Threshold	7	
EPSS Threshold	10%	
Catalogs to use	CERT-FR ALE	
NVD API Key		(get an API Key from https://nvd.nist.gov/developers/request-an-api-key)

README

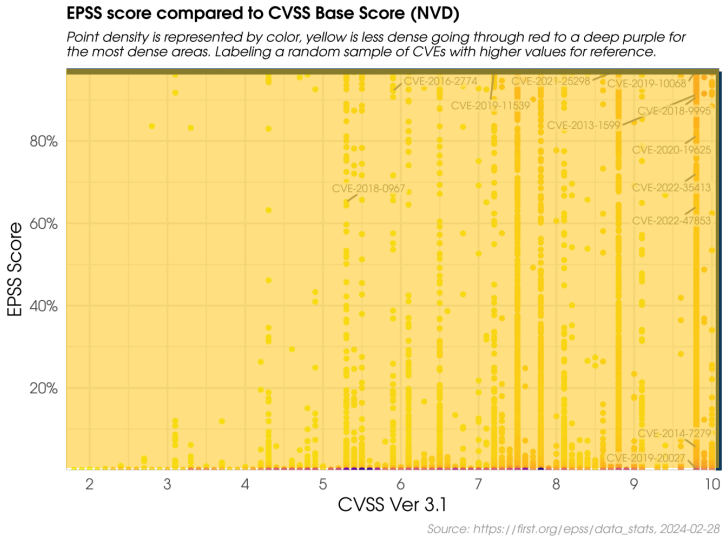
How to use this file:

1. Get your own API Key from NVD at https://nvd.nist.gov/developers/request-an-api-key
2. Enter your API Key in cell I4 (the black cell)
3. Set your thresholds in cells I1 and I2
4. Choose the catalogs to use in the I3 drop down
5. Enter the CVE you want to analyze in column A

Available for free here: https://share.cyberwatch.fr/s/xgqS8zXa727kbRn

Conclusion / Use case:
How to give hope to your Vulnerability Management team?

Implement this on all your devices

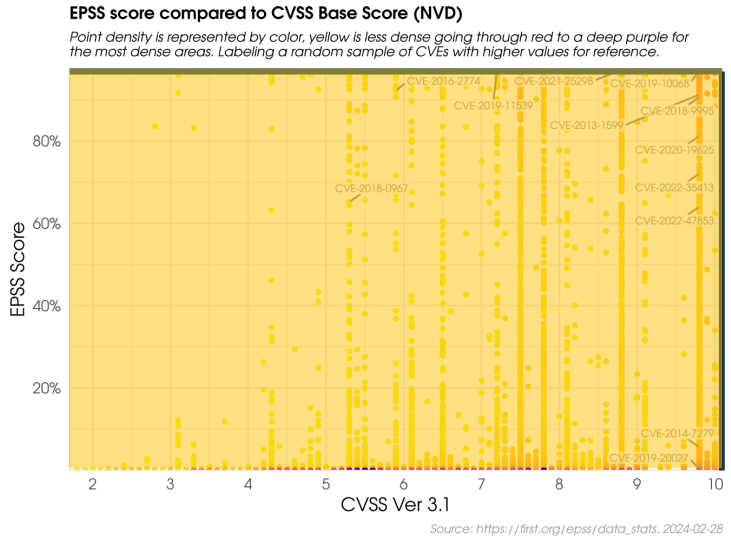


CVSS > 10
EPSS > 100%
+ CERT-FR ALE

Here, CVEs will be marked as high priority only if they have been cherry-picked by CERT-FR ALE

Conclusion / Use case:
How to give hope to your Vulnerability Management team?

Implement this on all your devices



CVSS > 10
EPSS > 100%
+ CERT-FR ALE

Here, CVEs will be marked as high priority only if they have been cherry-picked by CERT-FR ALE

Impact on the Vulnerability stats:

-90,3%

Impact on the Remediation plan:

Update Windows
Update.NET
Update Firefox
Update Adobe Acrobat
Update 7-Zip
Update the Linux kernel

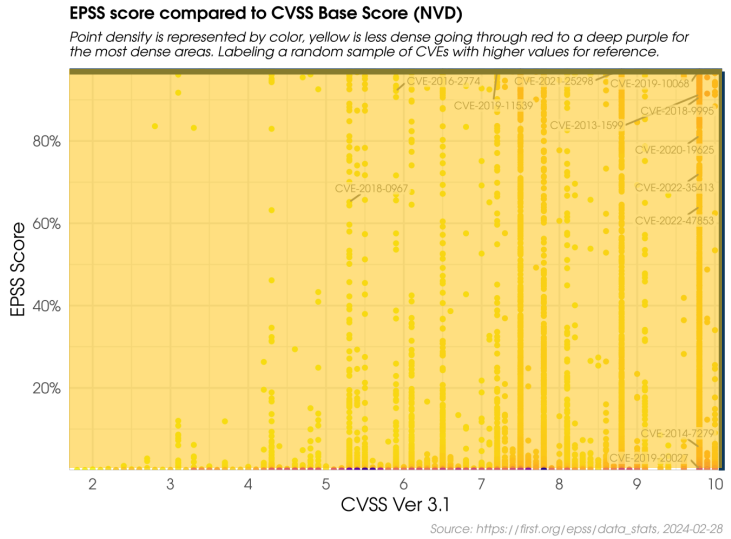
Only 1 action

Update Windows asap

Other patches can wait

Then, when you are ready to go further…

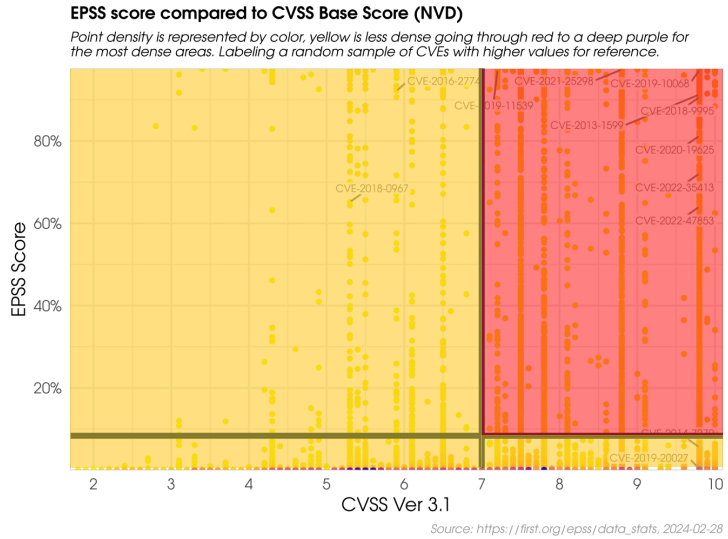
Implement this on all your devices



CVSS > 10
EPSS > 100%
+ CERT-FR ALE

Here, CVEs will be marked as high priority only if they have been cherry-picked by CERT-FR ALE

Critical assets



CVSS > 7
EPSS > 10%
+ CERT-FR ALE / CISA KEV

Q&A

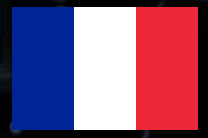
Thanks for your attention!

GALEAX – Vulnerability Management Expertise

maxime@galeax.com

+33 6 25 23 64 81

Platinum Cyberwatch Partner



French company

Référencé par UGAP

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

CLUSIF

UTILISÉ PAR LES ARMÉES FRANÇAISES