



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

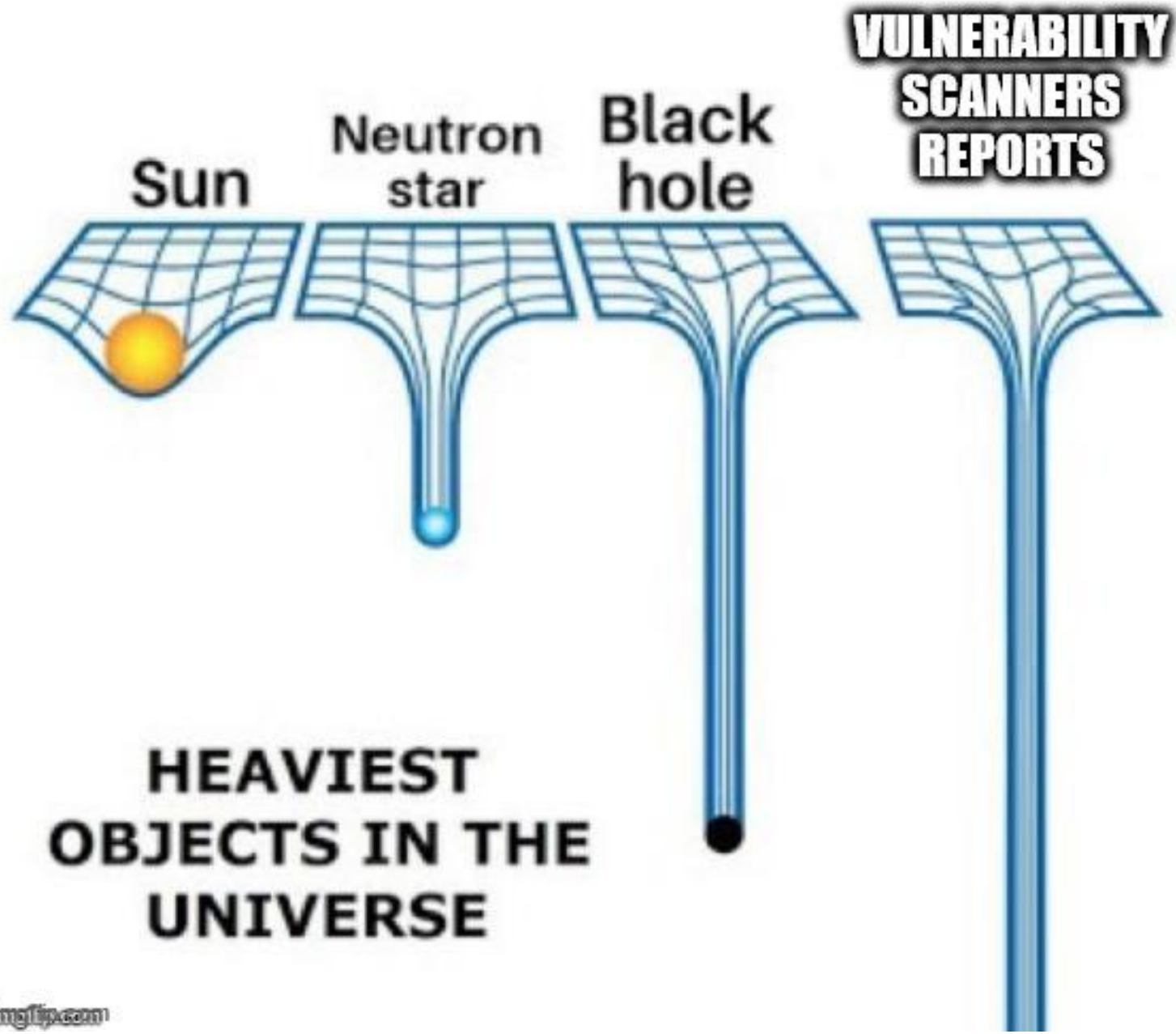
Co-founder of:

- Cyberwatch (acquired by **framatom**e in 2022)
- Galeax (Cyberwatch platinum partner) in 2023

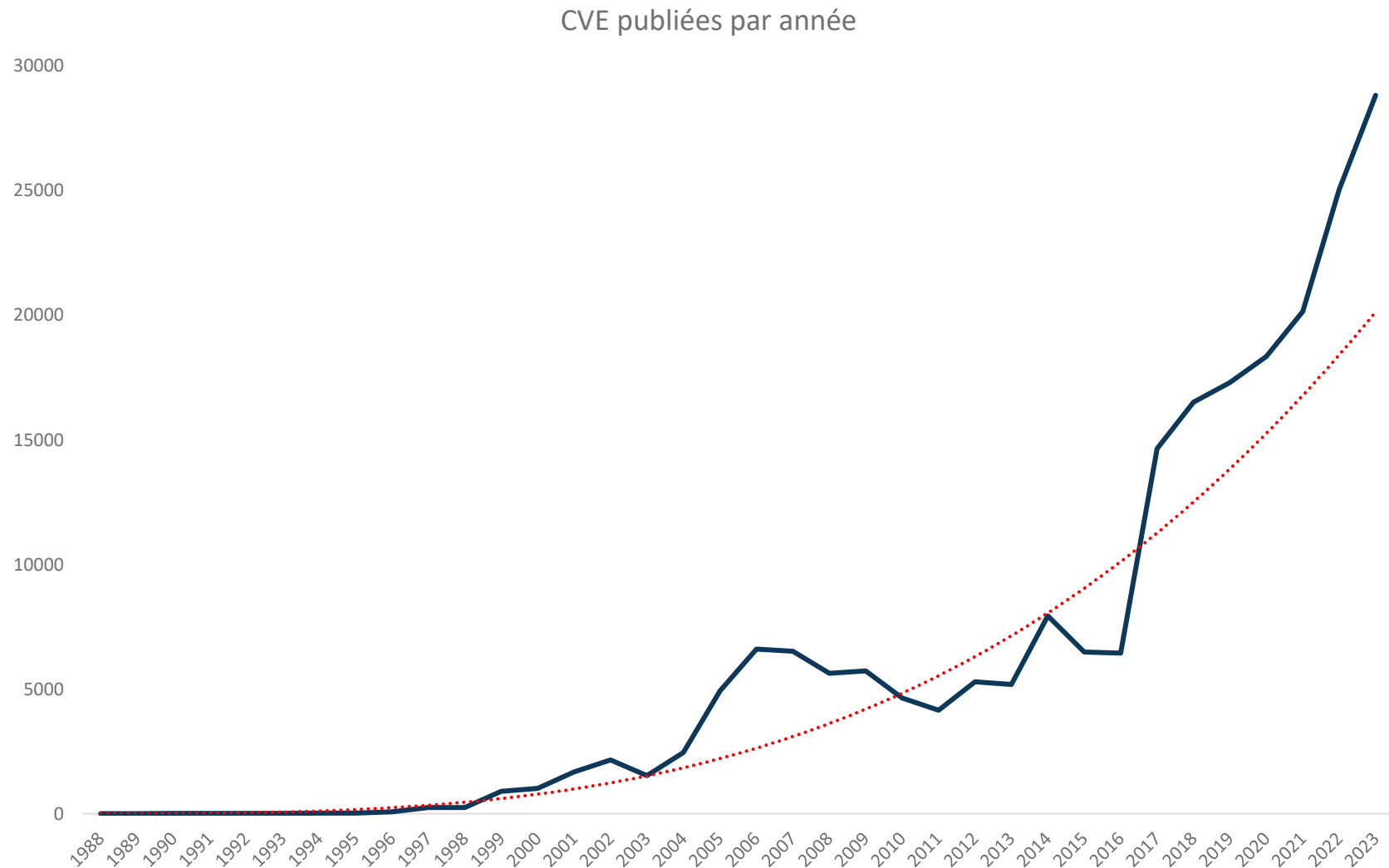


GALEAX

 **cyberwatch**



+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 Meta Temp Score [?]
3.6



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

8.3 (High)

Attack Vector (AV)
Network (N) Adjacent (A) Local (L) Physical (P) Changed (C)

Attack Complexity (AC)
Low (L) High (H) None (N) Low (L) High (H)

Privileges Required (PR)
None (N) Low (L) High (H)

User Interaction (UI)
None (N) Required (R)

Integrity (I)
None (N) Low (L) High (H)

Availability (A)
None (N) Low (L) High (H)

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

Temporal Score

7.6 (High)

Exploit Code Maturity (E)
Not Defined (X) Unproven (U) Proof-of-Concept (P) Functional (F) High (H)

Remediation Level (RL)
Not Defined (X) Official Fix (O) Temporary Fix (T) Workaround (W) Unavailable (U)

Report Confidence (RC)
Not Defined (X) Unknown (U) Reasonable (R) Confirmed (C)

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

Environmental Score

5.9 (Medium)

Confidentiality Requirement (CR)
Not Defined (X) Low (L) Medium (M) High (H)

Integrity Requirement (IR)
Not Defined (X) Low (L) Medium (M) High (H)

Availability Requirement (AR)
Not Defined (X) Low (L) Medium (M) High (H)

Modified Attack Vector (MAV)
Not Defined (X) Network (N) Adjacent Network (AN) Local (L) Physical (P)

Modified Attack Complexity (MAC)
Not Defined (X) Low (L) High (H)

Modified Privileges Required (MPR)
Not Defined (X) None (N) Low (L) High (H)

Modified User Interaction (MUI)
Not Defined (X) None (N) Required (R)

Modified Scope (MS)
Not Defined (X) Unchanged (U) Changed (C)

Modified Confidentiality (MC)
Not Defined (X) None (N) Low (L) High (H)

Modified Integrity (MI)
Not Defined (X) None (N) Low (L) High (H)

Modified Availability (MA)
Not Defined (X) None (N) Low (L) High (H)

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

Base Score **8.3**
(High)

Attack Vector (AV)

Attack Complexity (AC)

Privileges Required (PR)

User Interaction (UI)

Scope (S)

Confidentiality (C)

Integrity (I)

Availability (A)

Temporal Score **7.6**
(High)

Exploit Code Maturity (E)

Remediation Level (RL)

Report Confidence (RC)

Environmental Score **5.9**
(Medium)

Confidentiality Requirement (CR)

Integrity Requirement (IR)

Availability Requirement (AR)

Modified Attack Vector (MAV)

Modified Attack Complexity (MAC)

Modified Privileges Required (MPR)

Modified User Interaction (MUI)

Modified Scope (MS)

Modified Confidentiality (MC)

Modified Integrity (MI)

Modified Availability (MA)

11 parameters to adjust for each asset or each set of assets!

Note: CVSSv4 will not make the situation easier

Base Metrics ?

Exploitability Metrics

Attack Vector (AV):	<input checked="" type="radio"/> Network (N)	<input type="radio"/> Adjacent (A)	<input type="radio"/> Local (L)	<input type="radio"/> Physical (P)
Attack Complexity (AC):	<input checked="" type="radio"/> Low (L)	<input type="radio"/> High (H)		
Attack Requirements (AT):	<input checked="" type="radio"/> None (N)	<input type="radio"/> Present (P)		
Privileges Required (PR):	<input checked="" type="radio"/> None (N)	<input type="radio"/> Low (L)	<input type="radio"/> High (H)	
User Interaction (UI):	<input checked="" type="radio"/> None (N)	<input type="radio"/> Passive (P)	<input type="radio"/> Active (A)	

Vulnerable System Impact Metrics

Confidentiality (VC):	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input checked="" type="radio"/> None (N)
Integrity (VI):	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input checked="" type="radio"/> None (N)
Availability (VA):	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input checked="" type="radio"/> None (N)

Subsequent System Impact Metrics

Confidentiality (SC):	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input checked="" type="radio"/> None (N)
Integrity (SI):	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input checked="" type="radio"/> None (N)
Availability (SA):	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input checked="" type="radio"/> None (N)

Environmental (Security Requirements) ?

Confidentiality Requirements (CR):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> High (H)	<input type="radio"/> Medium (M)	<input type="radio"/> Low (L)
Integrity Requirements (IR):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> High (H)	<input type="radio"/> Medium (M)	<input type="radio"/> Low (L)
Availability Requirements (AR):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> High (H)	<input type="radio"/> Medium (M)	<input type="radio"/> Low (L)

Threat Metrics ?

Exploit Maturity (E):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Attacked (A)	<input type="radio"/> POC (P)	<input type="radio"/> Unreported (U)
-----------------------	--	------------------------------------	-------------------------------	--------------------------------------

Supplemental Metrics ?

Safety (S):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Negligible (N)	<input type="radio"/> Present (P)		
Automatable (AU):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> No (N)	<input type="radio"/> Yes (Y)		
Recovery (R):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Automatic (A)	<input type="radio"/> User (U)	<input type="radio"/> Irrecoverable (I)	
Value Density (V):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Diffuse (D)	<input type="radio"/> Concentrated (C)		
Vulnerability Response Effort (RE):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Low (L)	<input type="radio"/> Moderate (M)	<input type="radio"/> High (H)	
Provider Urgency (U):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Clear	<input type="radio"/> Green	<input type="radio"/> Amber	<input type="radio"/> Red

Environmental (Modified Base Metrics) ?

Exploitability Metrics

Attack Vector (MAV):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Network (N)	<input type="radio"/> Adjacent (A)	<input type="radio"/> Local (L)	<input type="radio"/> Physical (P)
Attack Complexity (MAC):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Low (L)	<input type="radio"/> High (H)		
Attack Requirements (MAT):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> None (N)	<input type="radio"/> Present (P)		
Privileges Required (MPR):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> None (N)	<input type="radio"/> Low (L)	<input type="radio"/> High (H)	
User Interaction (MUI):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> None (N)	<input type="radio"/> Passive (P)	<input type="radio"/> Active (A)	

Vulnerable System Impact Metrics

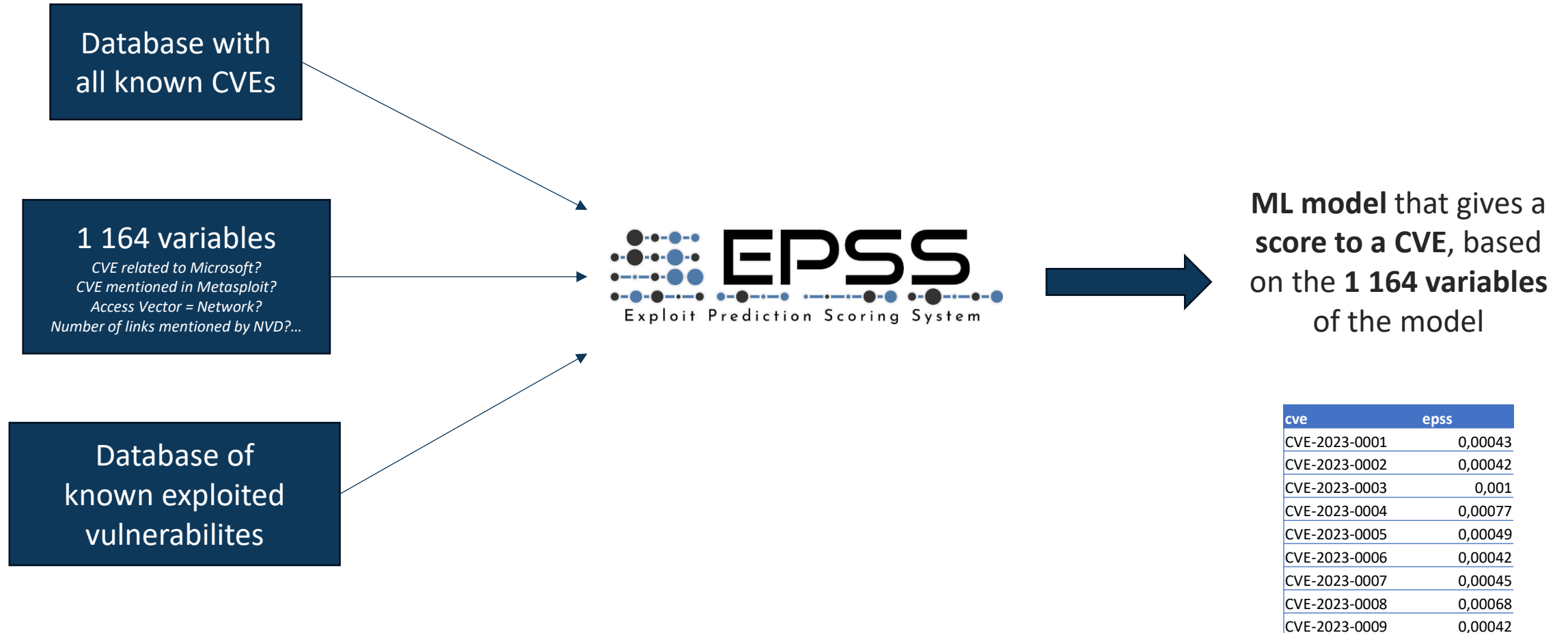
Confidentiality (MVC):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input type="radio"/> None (N)
Integrity (MVI):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input type="radio"/> None (N)
Availability (MVA):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input type="radio"/> None (N)

Subsequent System Impact Metrics

Confidentiality (MSC):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input type="radio"/> Negligible (N)	
Integrity (MSI):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Safety (S)	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input type="radio"/> Negligible (N)
Availability (MSA):	<input checked="" type="radio"/> Not Defined (X)	<input type="radio"/> Safety (S)	<input type="radio"/> High (H)	<input type="radio"/> Low (L)	<input type="radio"/> Negligible (N)

New environmental parameters

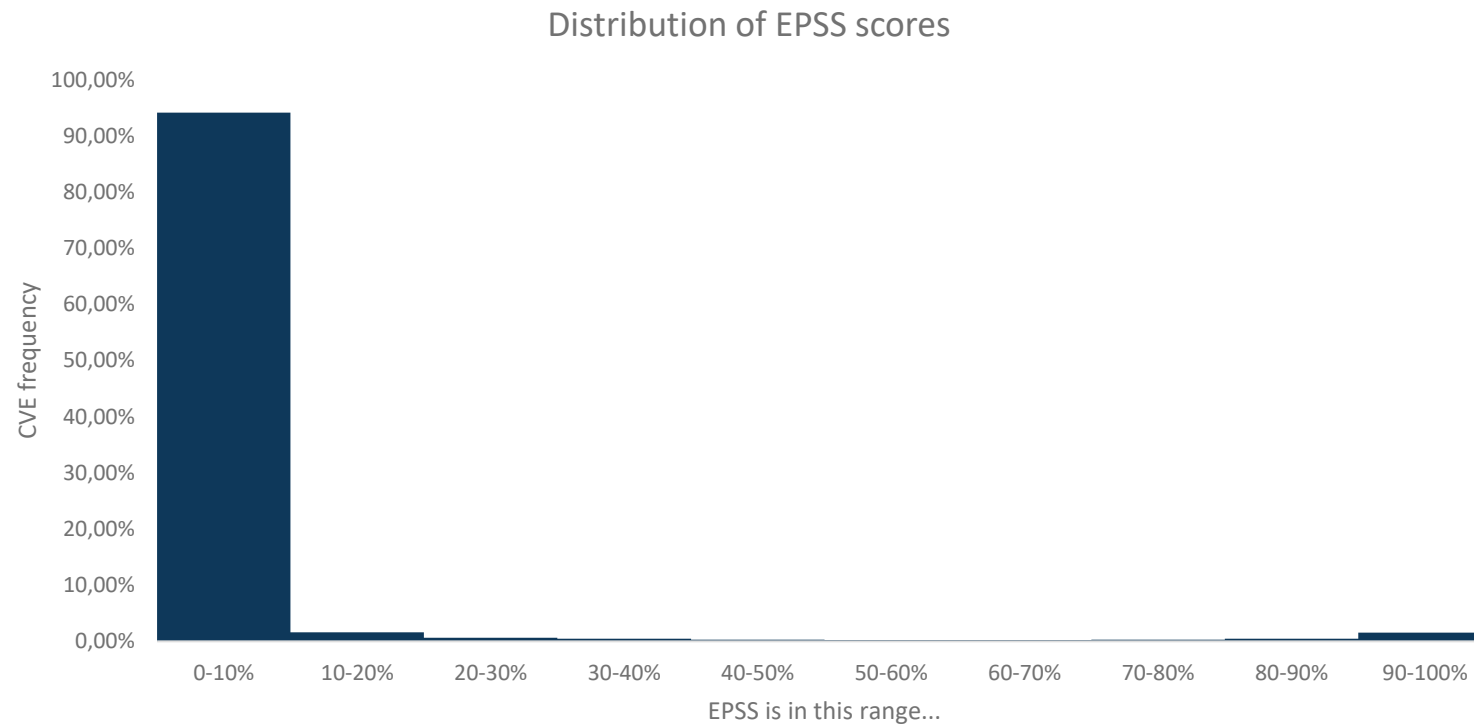
A new score has been released in 2023: EPSSv3



EPSS can eliminate most vulnerabilities

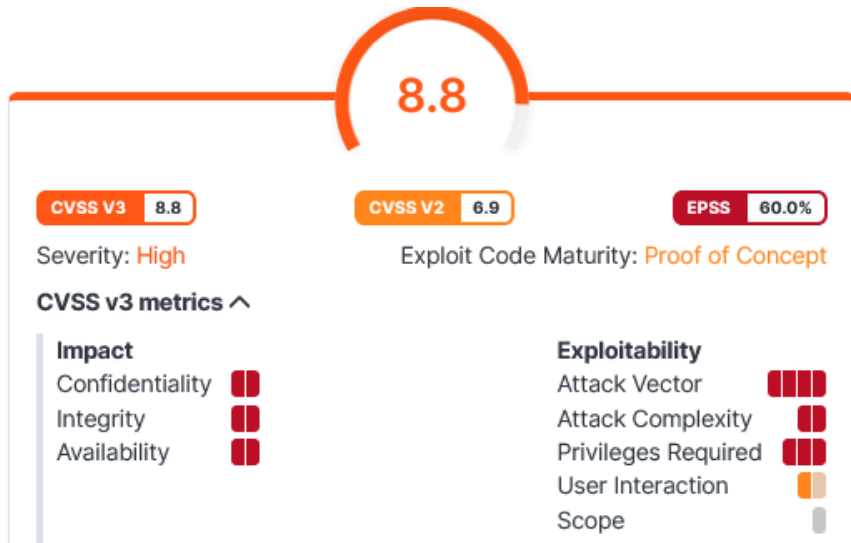
Filtering CVEs with **EPSS < 20%** will actually **remove 95%** of them!

Median: 0.143% - Mean: 3.59%



Limit #3 : EPSSv3 is not « magical »

CVE-2020-0801

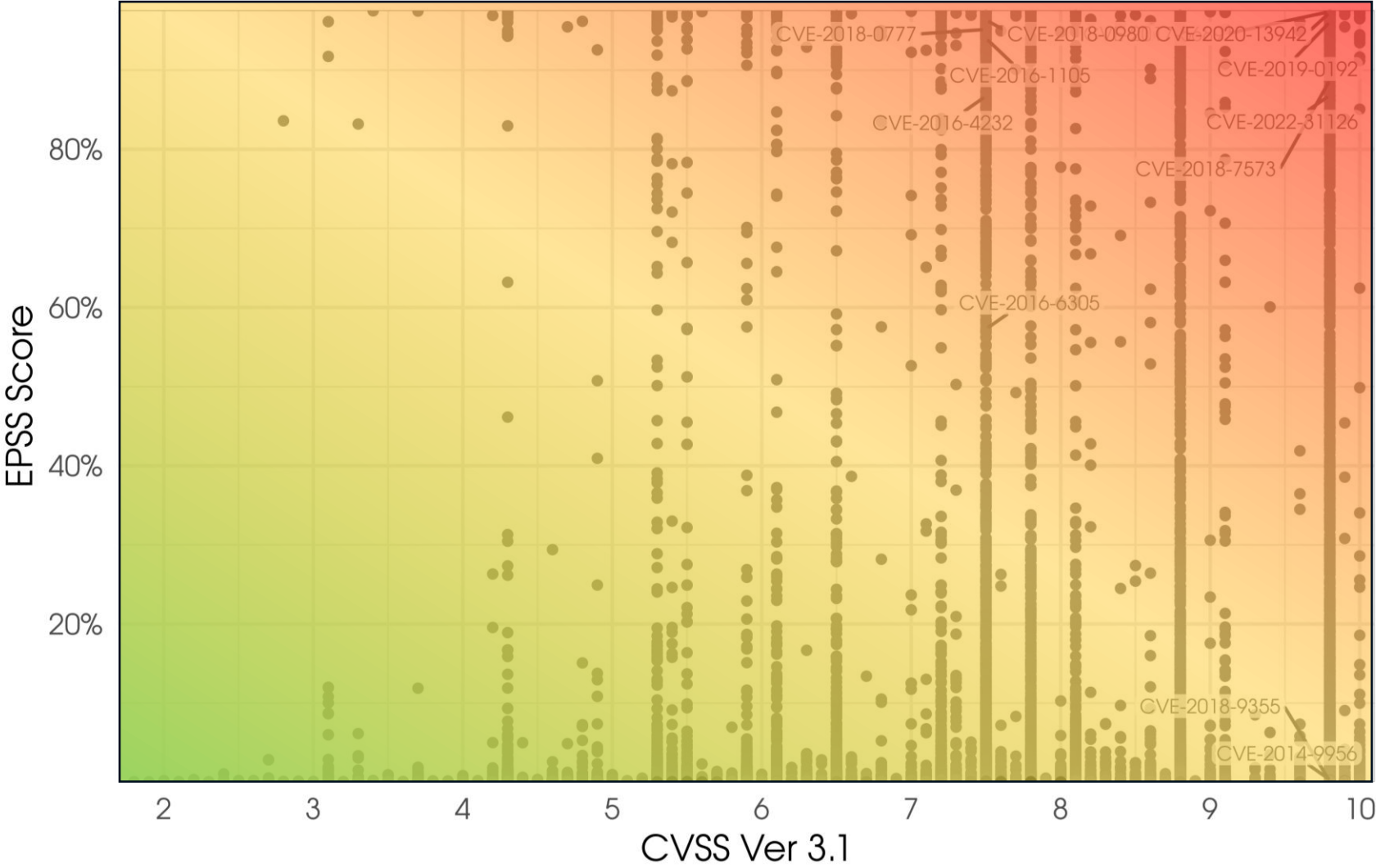


Publicly disclosed	Exploited	Exploitability assessment
No	No	Exploitation Less Likely

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

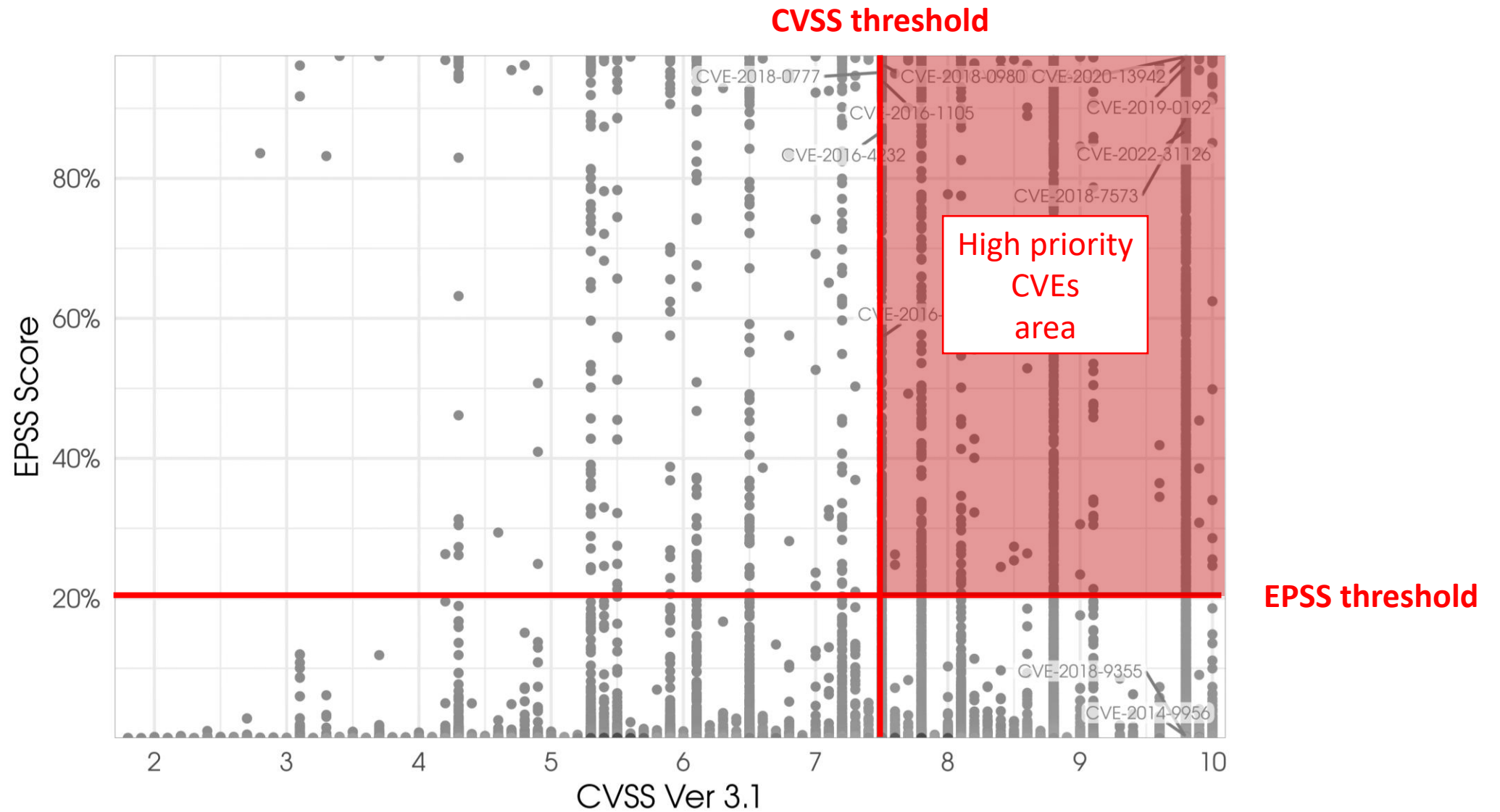
Root cause: EPSS is very influenced by the vendor of the vulnerable technology
(Microsoft => very high EPSS)

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

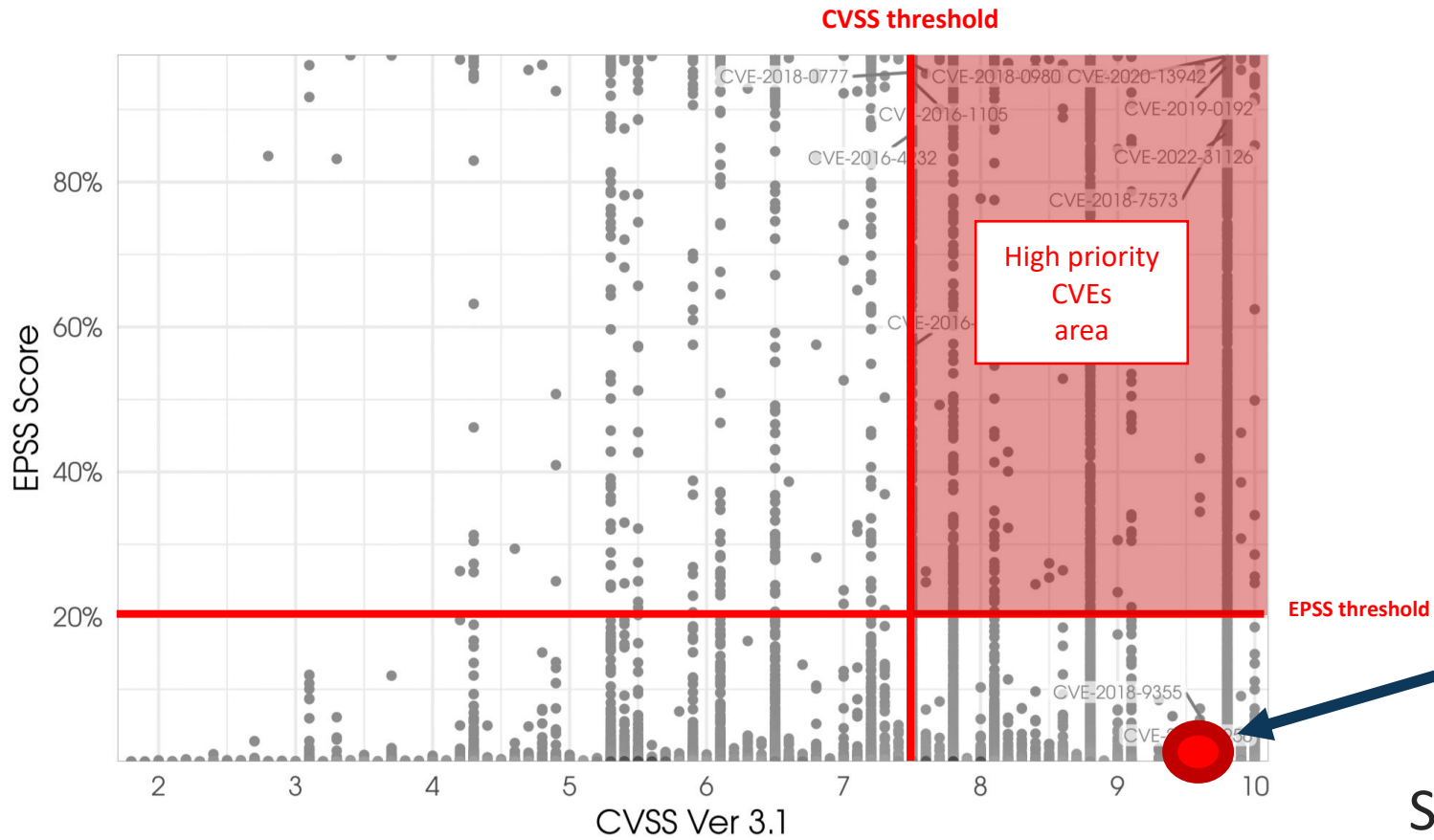


Source: https://first.org/epss/data_stats, 2024-03-26

Proposal: combine CVSS & EPSS to better sort your CVEs



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

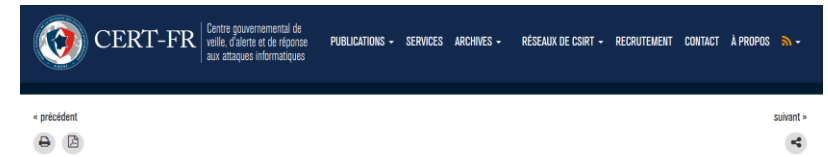


Source: https://first.org/epss/data_stats, 2024-03-26

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



Known Exploited Vulnerabilities Catalog



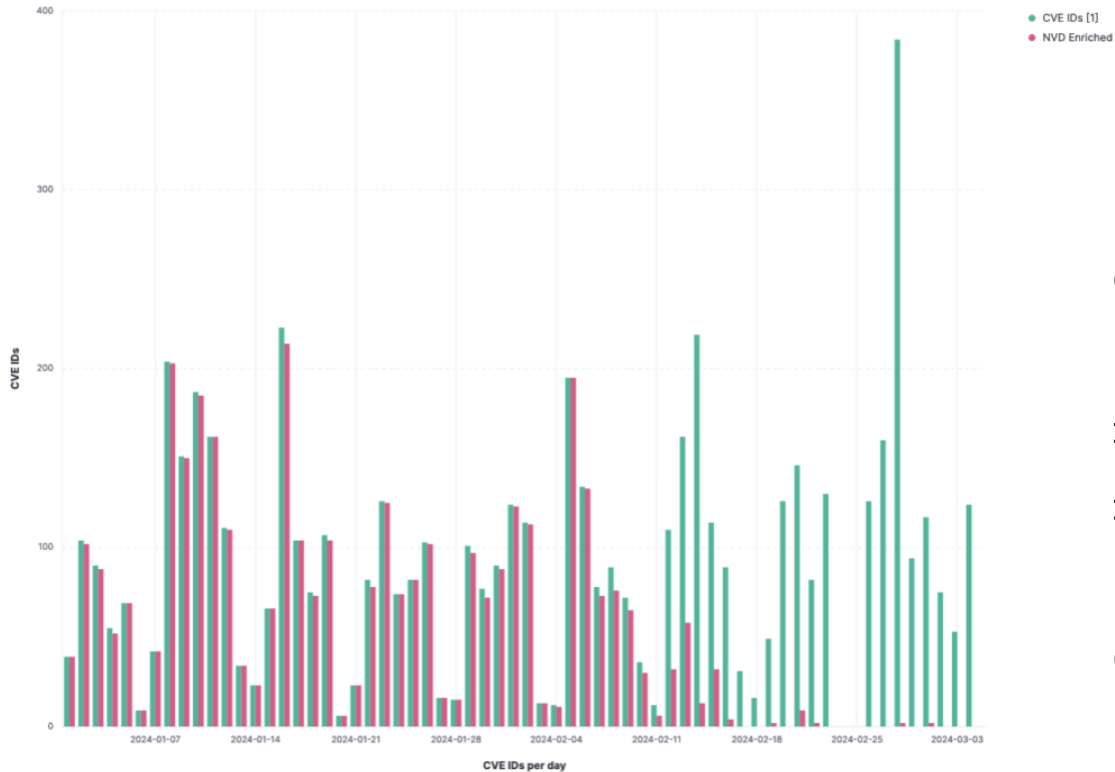
BULLETIN D'ALERTE DU CERT-FR

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)

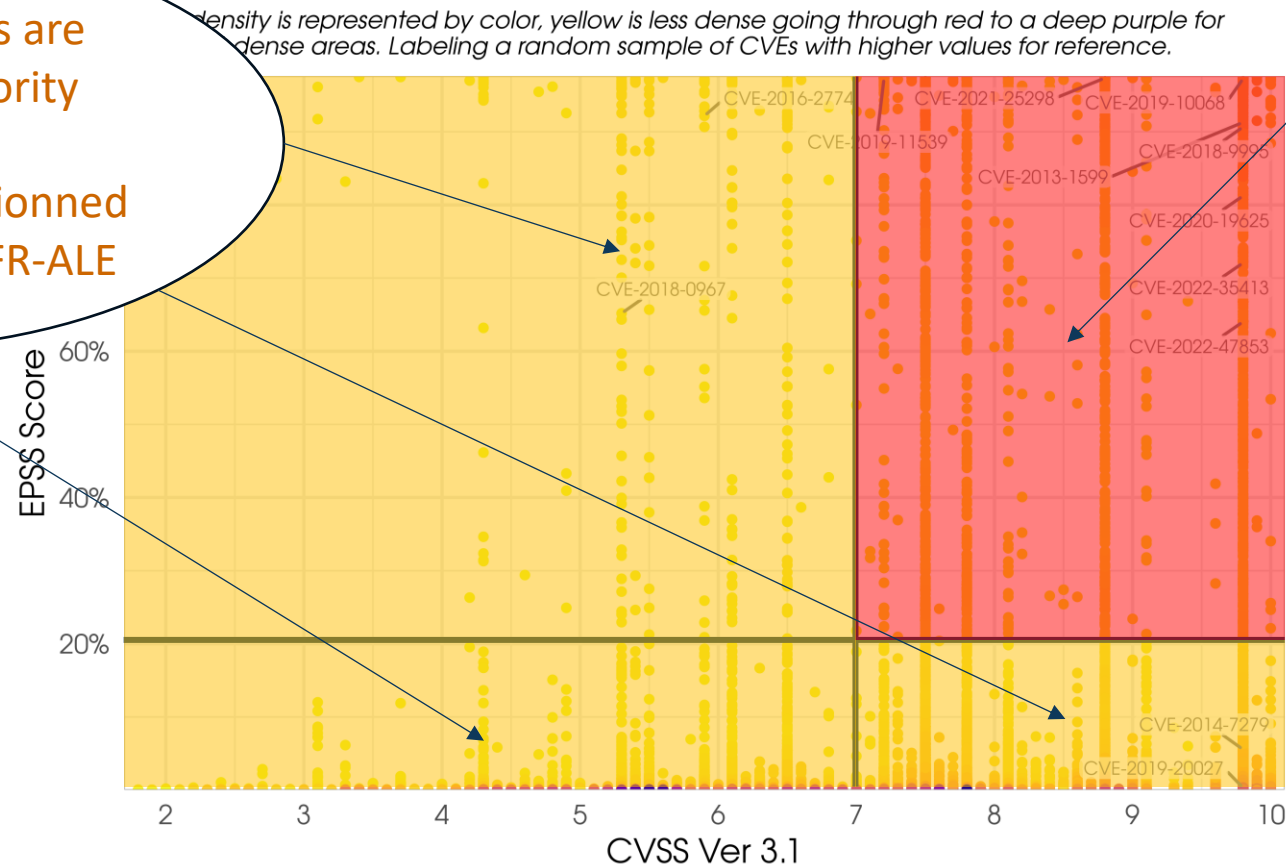
Can not plot these CVEs on the CVSS/EPSS graph!

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 mentioned by CISA KEV or CERTFR-ALE

EPSS score compared to CVSS Base Score (NVD)



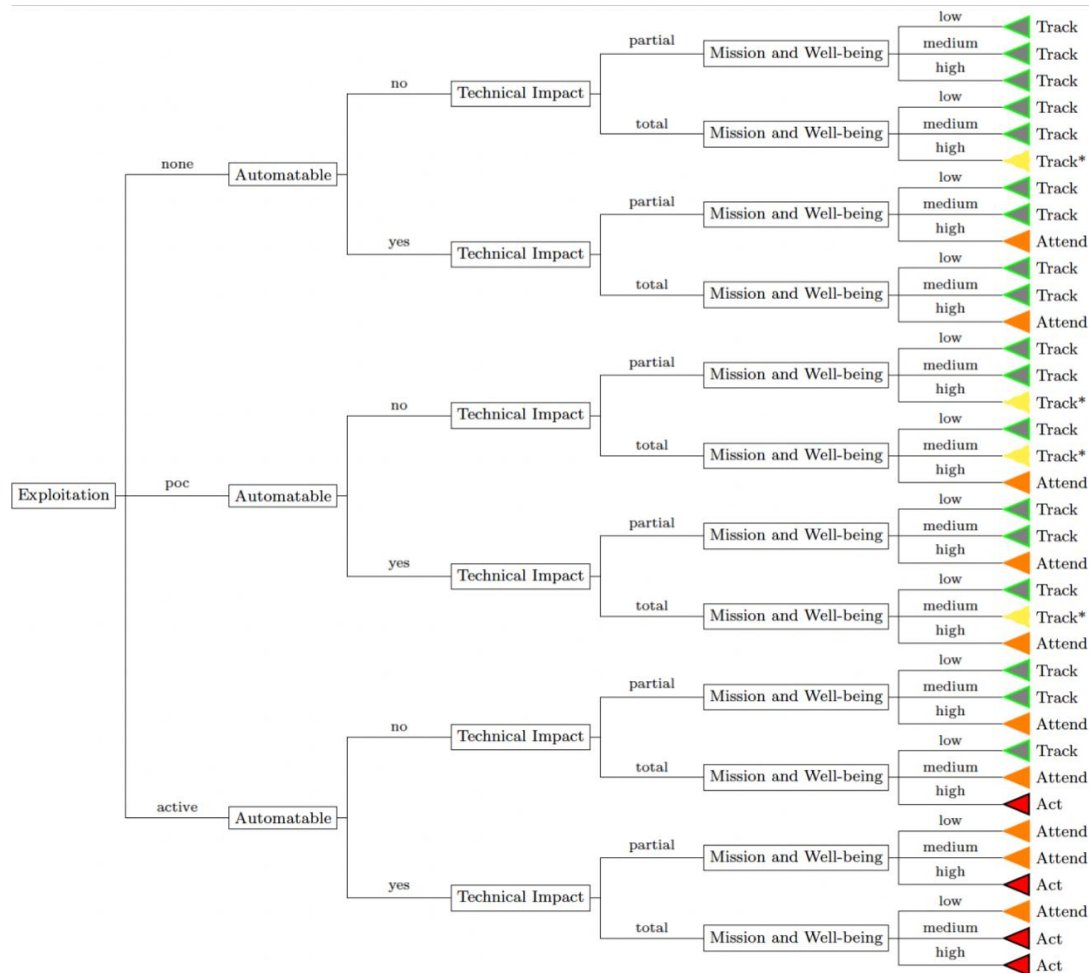
CVE here have high priority (both CVSS & EPSS thresholds have been reached)

Source: https://first.org/epss/data_stats, 2024-02-28

Remark #1: what about SSSVC?



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 ?

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (0/3)	Acquire Access (0/3)	Content Injection (0/3)	Cloud Administration Command (0/3)	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal (0/1)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise (0/3)	Command and Scripting Interpreter (0/10)	BITS Jobs (0/6)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery (0/5)	Internal Spearphishing (0/3)	Archive Collected Data (0/3)	Communication Through Removable Media (0/3)	Data Transfer Size Limits (0/3)	Data Destruction (0/3)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application (0/8)	Container Administration Command (0/5)	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	BITS Jobs (0/5)	Credentials from Password Stores (0/6)	Browser Information Discovery (0/2)	Lateral Tool Transfer (0/2)	Audio Capture (0/2)	Content Injection (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact (0/2)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services (0/4)	Deploy Container (0/3)	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/6)	Build Image on Host (0/3)	Exploitation for Credential Access (0/3)	Cloud Infrastructure Discovery (0/3)	Remote Service Session Hijacking (0/2)	Automated Collection (0/3)	Data Encoding (0/2)	Exfiltration Over C2 Channel (0/3)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions (0/4)	Exploitation for Client Execution (0/3)	Browser Extensions (0/3)	Boot or Logon Autostart Execution (0/14)	Debugger Evasion (0/2)	Forced Authentication (0/2)	Cloud Service Dashboard (0/2)	Remote Services (0/3)	Browser Session Hijacking (0/3)	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Host Software Binary (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information (0/4)	Forge Web Credentials (0/2)	Cloud Service Discovery (0/4)	Replication Through Removable Media (0/3)	Clipboard Data (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media (0/3)	Native API (0/3)	Create Account (0/3)	Create or Modify System Process (0/5)	Deploy Container (0/2)	Input Capture (0/4)	Cloud Storage Object Discovery (0/2)	Software Deployment Tools (0/3)	Data from Cloud Storage (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Direct Volume Access (0/2)	Modify Authentication Process (0/9)	Container and Resource Discovery (0/3)	Taint Shared Content (0/4)	Data from Configuration Repository (0/2)	Fallback Channels (0/3)	Exfiltration Over Web Service (0/4)	Financial Theft (0/3)
Search Open Websites/Domains (0/3)	Trusted Relationship (0/4)	Serverless Execution (0/3)	Serverless Execution (0/3)	Event Triggered Execution (0/16)	Domain or Tenant Policy Modification (0/2)	Domain or Tenant Policy Modification (0/2)	Multi-Factor Authentication Interception (0/3)	Debugger Evasion (0/2)	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Hide Infrastructure (0/2)	Exfiltration Over Web Service (0/4)	Firmware Corruption (0/2)
Search Victim-Owned Websites (0/4)	Valid Accounts (0/4)	Shared Modules (0/2)	Shared Modules (0/2)	External Remote Services (0/13)	Escape to Host (0/16)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation (0/2)	Device Driver Discovery (0/2)	Data from Local System (0/2)	Data from Network Shared Drive (0/2)	Ingress Tool Transfer (0/2)	Scheduled Transfer (0/2)	Inhibit System Recovery (0/2)
		Software Deployment Tools (0/2)	Software Deployment Tools (0/2)	Hijack Execution Flow (0/13)	Event Triggered Execution (0/16)	Exploitation for Defense Evasion (0/13)	Network Sniffing (0/6)	Domain Trust Discovery (0/2)	Data from Network Shared Drive (0/2)	Data from Network Shared Drive (0/2)	Multi-Stage Channels (0/2)	Transfer Data to Cloud Account (0/2)	Network Denial of Service (0/2)
		System Services (0/3)	System Services (0/3)	Implant Internal Image (0/13)	Exploitation for Privilege Escalation (0/13)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery (0/2)	Data from Removable Media (0/2)	Data from Removable Media (0/2)	Non-Application Layer Protocol (0/2)	Transfer Data to Cloud Account (0/2)	Resource Hijacking (0/2)
		User Execution (0/9)	User Execution (0/9)	Modify Authentication Process (0/13)	Hijack Execution Flow (0/13)	Hide Artifacts (0/12)	Steal Application Access Token (0/12)	Group Policy Discovery (0/12)	Data Staged (0/2)	Data Staged (0/2)	Non-Standard Port (0/4)	Transfer Data to Cloud Account (0/2)	Service Stop (0/4)
		Windows Management Instrumentation (0/6)	Windows Management Instrumentation (0/6)	Office Application Startup (0/6)	Process Injection (0/12)	Hijack Execution Flow (0/6)	Steal or Forge Authentication Certificates (0/6)	Log Enumeration (0/6)	Email Collection (0/3)	Email Collection (0/3)	Proxy (0/4)	Transfer Data to Cloud Account (0/2)	System Shutdown/Reboot (0/4)
									Input Capture (0/3)	Input Capture (0/3)	Remote Access Software (0/3)	Transfer Data to Cloud Account (0/2)	
											Traffic Signaling (0/3)		

Attack path

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

Cyberwatch export

selection controls layer controls technique controls

push_pin

Initial Access 10 techniques	Execution 12 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 41 techniques	Credential Access 17 techniques	Discovery 28 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 18 techniques	Exfiltration 8 techniques	Impact 14 techniques
Phishing (3/4)	Software Deployment Tools	Hijack Execution Flow (11/13)	Access Token Manipulation (3/5)	Access Token Manipulation (3/5)	Steal Web Session Cookie	File and Directory Discovery	Use Alternate Authentication Material (3/3)	Adversary-in-the-Middle (2/3)	Proxy (2/4)	Automated Exfiltration (0/1)	Endpoint Denial of Service (4/4)
Valid Accounts (1/3)	Command and Scripting Interpreter (0/9)	Create or Modify System Process (3/5)	Hijack Execution Flow (11/13)	Use Alternate Authentication Material (3/3)	Steal Application Access Token	Network Sniffing	Taint Shared Content	Data from Local System	Application Layer Protocol (0/4)	Data Transfer Size Limits	Data Manipulation (1/3)
External Remote Services	Container Administration Command	Event Triggered Execution (4/16)	Create or Modify System Process (3/5)	Impair Defenses (5/9)	Forge Web Credentials (1/2)	Account Discovery (0/3)	Remote Service Session Hijacking (0/2)	Browser Session Hijacking	Communication Through Removable Media	Exfiltration Over Alternative Protocol (0/3)	Network Denial of Service (2/2)
Supply Chain Compromise (2/3)	Deploy Container	Boot or Logon Autostart Execution (5/14)	Event Triggered Execution (4/16)	Hijack Execution Flow (11/13)	Modify Authentication Process (1/8)	Browser Information Discovery	Internal Spearphishing	Input Capture (1/4)	Content Injection	Exfiltration Over C2 Channel	Defacement (0/2)
Content Injection	Exploitation for Client Execution	Modify Authentication Process (1/8)	Boot or Logon Autostart Execution (5/14)	Obfuscated Files or Information (2/13)	Network Sniffing	Group Policy Discovery	Remote Services (1/6)	Email Collection (1/3)	Data Encoding (0/2)	Account Access Removal	
Drive-by Compromise	Inter-Process Communication (0/3)	Pre-OS Boot (2/5)	Boot or Logon Initialization Scripts (0/5)	Subvert Trust Controls (2/6)	Multi-Factor Authentication Interception	Network Service Discovery	Software Deployment Tools	Automated Collection	Data Obfuscation (0/3)	Data Destruction	
Exploit Public-Facing Application	Native API	Server Software Component	Abuse Elevation Control Mechanism (1/5)	Masquerading (3/9)	Adversary-in-the-Middle (2/3)	Network Share Discovery	Exploitation of Remote Services	Data from Configuration Repository (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Data Encrypted for Impact
Hardware Additions	Scheduled Task/Job (0/5)	Boot or Logon Initialization Scripts (0/5)	Escape to Host	Modify Authentication Process (1/8)	Unsecured Credentials (5/6)	Peripheral Device Discovery	Lateral Tool Transfer	Data from Information Repositories (0/1)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Replication Through Removable Media	Shared Modules	Compromise Host Software Binary	Valid Accounts (1/3)	Pre-OS Boot (2/5)	Input Capture (1/4)	Permission Groups Discovery (0/2)	Replication Through Removable Media	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (0/4)	Financial Theft
Trusted Relationship	System Services (0/2)	Valid Accounts (1/3)	Process Injection (0/12)	Rootkit	Brute Force (4/4)	Process Discovery		Archive Collected Data (0/3)	Hide Infrastructure	Scheduled Transfer	Firmware Corruption
	User Execution (0/3)	External Remote Services	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (1/5)	Steal or Forge Kerberos Tickets (1/5)	Remote System Discovery		Audio Capture	Ingress Tool Transfer		Inhibit System Recovery
	Windows Management Instrumentation	Browser Extensions	Domain or Tenant Policy Modification (0/2)	Exploitation for Defense Evasion	Credentials from Password Stores (1/5)	System Information Discovery		Clipboard Data	Multi-Stage Channels		Resource Hijacking
		Account Manipulation (0/4)	Hide Artifacts (1/12)	Hide Artifacts (1/12)	OS Credential Dumping (0/8)	System Network Configuration Discovery (0/2)		Data from Removable Media	Non-Application Layer Protocol		Service Stop
		BITS Jobs	Valid Accounts (1/3)	Valid Accounts (1/3)	Exploitation for Credential Access	System Network Connections Discovery		Data Staged (0/2)	Non-Standard Port		System Shutdown/Reboot
		Create Account (0/2)	Exploitation for Privilege Escalation	Reflective Code Loading	Forced Authentication	System Owner/User Discovery		Screen Capture	Protocol Tunneling		
		Implant Internal Image	Scheduled Task/Job (0/5)	Process Injection (0/12)	Multi-Factor Authentication	System Service Discovery		Video Capture	Remote Access Software		
		Office Application Startup		Indicator Removal					Traffic Signaling (0/2)		
									Web Service (0/3)		

Classical approach: target the earliest steps of an attack

Cyberwatch export

selection controls layer controls technique controls

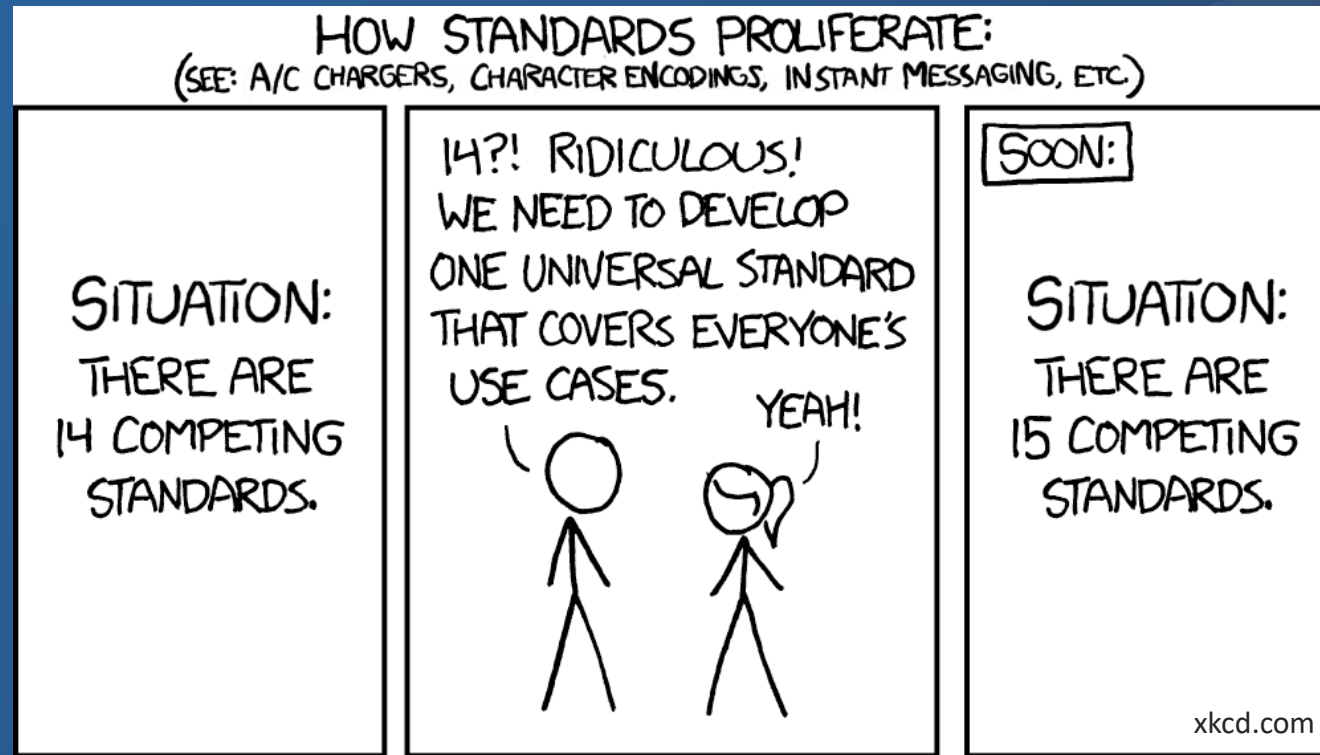
push_pin

Initial Access 10 techniques	Execution 12 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 41 techniques	Credential Access 17 techniques	Discovery 28 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 18 techniques	Exfiltration 8 techniques	Impact 14 techniques
Phishing (3/4)	Software Deployment Tools	Attack Execution Flow (11/13)	Access Token Manipulation (3/5)	Access Token Manipulation (3/5)	Steal Web Session Cookie	File and Directory Discovery	Use Alternate Authentication Material (3/3)	Adversary-in-the-Middle (2/3)	Proxy (2/4)	Automated Exfiltration (0/1)	Endpoint Denial of Service (4/4)
Valid Accounts (1/3)	Command and Scripting Interpreter (0/9)	Create or Modify System Process (3/5)	Hijack Execution Flow (11/13)	Use Alternate Authentication Material (3/3)	Steal Application Access Token	Network Sniffing	Taint Shared Content	Data from Local System	Application Layer Protocol (0/4)	Data Transfer Size Limits (1/3)	Data Manipulation (1/3)
External Remote Services	Container Administration Command	Event Triggered Execution (4/16)	Create or Modify System Process (3/5)	Impair Defenses (5/9)	Forge Web Credentials (1/2)	Account Discovery (0/3)	Remote Service Session Hijacking (0/2)	Browser Session Hijacking	Communication Through Removable Media	Exfiltration Over Alternative Protocol (0/3)	Network Denial of Service (2/2)
Supply Chain Compromise (2/3)	Deploy Container	Boot or Logon Autostart Execution (4/14)	Event Triggered Execution (4/16)	Hijack Execution Flow (11/13)	Modify Authentication Process (1/8)	Browser Information Discovery	Internal Spearphishing	Input Capture (1/4)	Content Injection	Exfiltration Over C2 Channel	Defacement (0/2)
Content Injection	Exploitation for Client Execution	Modify Authentication Process (1/8)	Boot or Logon Autostart Execution (5/14)	Obfuscated Files or Information (2/13)	Network Sniffing	Group Policy Discovery	Remote Services (1/6)	Email Collection (1/3)	Data Encoding (0/2)	Account Access Removal	
Drive-by Compromise	Inter-Process Communication (0/3)	Pre-OS Boot (2/5)	Boot or Logon Initialization Scripts (0/5)	Subvert Trust Controls (2/6)	Multi-Factor Authentication Interception	Network Service Discovery	Software Deployment Tools	Automated Collection	Data Obfuscation (0/3)	Data Destruction	
Exploit Public-Facing Application	Native API	Server Software Component (3/5)	Abuse Elevation Control Mechanism (1/5)	Masquerading (3/9)	Adversary-in-the-Middle (2/3)	Network Share Discovery	Exploitation of Remote Services	Data from Configuration Repository (0/2)	Dynamic Resolution (0/3)	Data Encrypted for Impact	
Hardware Additions	Scheduled Task/Job (0/5)	Boot or Logon Initialization Scripts (0/5)	Escape to Host	Modify Authentication Process (1/8)	Unsecured Credentials (5/6)	Peripheral Device Discovery	Lateral Tool Transfer	Data from Information Repositories (0/1)	Encrypted Channel (0/2)	Disk Wipe (0/2)	
Replication Through Removable Media	Shared Modules	Compromise Host Software Binary	Valid Accounts (1/3)	Pre-OS Boot (2/5)	Input Capture (1/4)	Permission Groups Discovery (0/2)	Replication Through Removable Media	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (0/4)	Financial Theft
Trusted Relationship	System Services (0/2)	Valid Accounts (1/3)	Process Injection (0/12)	Rootkit	Brute Force (4/4)	Process Discovery		Archive Collected Data (0/3)	Hide Infrastructure	Scheduled Transfer	Firmware Corruption
	User Execution (0/3)	External Remote Services	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (1/5)	Steal or Forge Kerberos Tickets (1/5)	Remote System Discovery		Audio Capture	Ingress Tool Transfer		Inhibit System Recovery
	Windows Management Instrumentation	Browser Extensions	Domain or Tenant Policy Modification (0/2)	Exploitation for Defense Evasion	Credentials from Password Stores (1/5)	System Information Discovery		Clipboard Data	Multi-Stage Channels		Resource Hijacking
		Account Manipulation (0/4)	Hide Artifacts (1/12)	Hide Artifacts (1/12)	OS Credential Dumping (0/8)	System Network Configuration Discovery (0/2)		Data from Removable Media	Non-Application Layer Protocol		Service Stop
		BITS Jobs	Valid Accounts (1/3)	Valid Accounts (1/3)	Exploitation for Credential Access	System Network Connections Discovery		Data Staged (0/2)	Non-Standard Port		System Shutdown/Reboot
		Create Account (0/2)	Exploitation for Privilege Escalation	Reflective Code Loading	Forced Authentication	System Owner/User Discovery		Screen Capture	Protocol Tunneling		
		Implant Internal Image	Scheduled Task/Job (0/5)	Process Injection (0/12)	Multi-Factor Authentication	System Service Discovery		Video Capture	Remote Access Software		
		Office Application Startup		Indicator Removal					Traffic Signaling (0/2)		
									Web Service (0/3)		

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 »

Initial Access 10 techniques	Execution 12 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 41 techniques	Credential Access 17 techniques	Discovery 28 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 18 techniques	Exfiltration 8 techniques	Impact 14 techniques
Content Injection	Command and Scripting Interpreter	Account Manipulation (0/4)	Access Token Manipulation (3/5)	Access Token Manipulation (3/5)	Forge Web Credentials (0/2)	Account Discovery (0/3)	Use Alternate Authentication Material (0/3)	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Drive-by Compromise	Container Administration Command	BITS Jobs	Abuse Elevation Control Mechanism (0/5)	Use Alternate Authentication Material (0/3)	Steal Application Access Token	Application Window Discovery	Exploitation of Remote Services	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploit Public-Facing Application	Deploy Container	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/5)	Steal Web Session Cookie	Browser Information Discovery	Internal Spearphishing	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
External Remote Services	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Adversary-in-the-Middle (0/3)	Container and Resource Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Hardware Additions	Inter-Process Communication (0/3)	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Brute Force (0/4)	Debugger Evasion	Remote Service Session Hijacking (0/2)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing (0/4)	Native API	Compromise Host Software Binary	Event Triggered Execution (0/16)	Debugger Evasion	Credentials from Password Stores (0/5)	Device Driver Discovery	Remote Services (0/6)	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Replication Through Removable Media	Scheduled Task/Job (0/5)	Create Account (0/2)	Create or Modify System Process (0/5)	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Domain Trust Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
Supply Chain Compromise (0/3)	Share Modules	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Deploy Container	Forced Authentication	File and Directory Discovery	Software Deployment Tools	Data from Information Repositories (0/1)	Fallback Channels	Scheduled Transfer	Financial Theft
Trusted Relationship	Software Deployment Tools	Event Triggered Execution (0/16)	Escape to Host	Direct Volume Access	Input Capture (0/4)	Group Policy Discovery	Taint Shared Content	Data from Local System	Hide Infrastructure		Firmware Corruption
Valid Accounts (0/3)	System Services (0/2)	External Remote Services	Event Triggered Execution (0/16)	Domain or Tenant Policy Modification (0/2)	Modify Authentication Process (0/8)	Log Enumeration		Data from Network Shared Drive	Ingress Tool Transfer		Inhibit System Recovery
	User Execution (0/3)	Hijack Execution Flow (0/13)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Network Service Discovery		Data from Removable Media	Multi-Stage Channels		Network Denial of Service (0/2)
	Windows Management Instrumentation	Implant Internal Image	Hijack Execution Flow (0/13)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Network Share Discovery		Data Staged (0/2)	Non-Application Layer Protocol		Resource Hijacking
		Modify Authentication Process (0/8)	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	Network Sniffing	Network Sniffing		Email Collection (0/3)	Non-Standard Port		Service Stop
		Office Application Startup (0/6)	Scheduled Task/Job (0/5)	Hide Artifacts (0/12)	OS Credential Dumping (0/8)	Password Policy Discovery		Input Capture (0/4)	Protocol Tunneling		System Shutdown/Reboot
		Power Settings	Valid Accounts (0/3)	Hijack Execution Flow (0/13)	Steal or Forge Authentication Certificates	Peripheral Device Discovery		Screen Capture	Proxy (0/4)		
		Pre-OS Boot (0/5)	Impair Defenses	Steal or Forge		Permission Groups Discovery (0/2)		Video Capture	Remote Access Software		
		Scheduled Task/Job				Process Discovery			Traffic Signaling (0/2)		
									Web Service (0/3)		



Pre-conclusion:

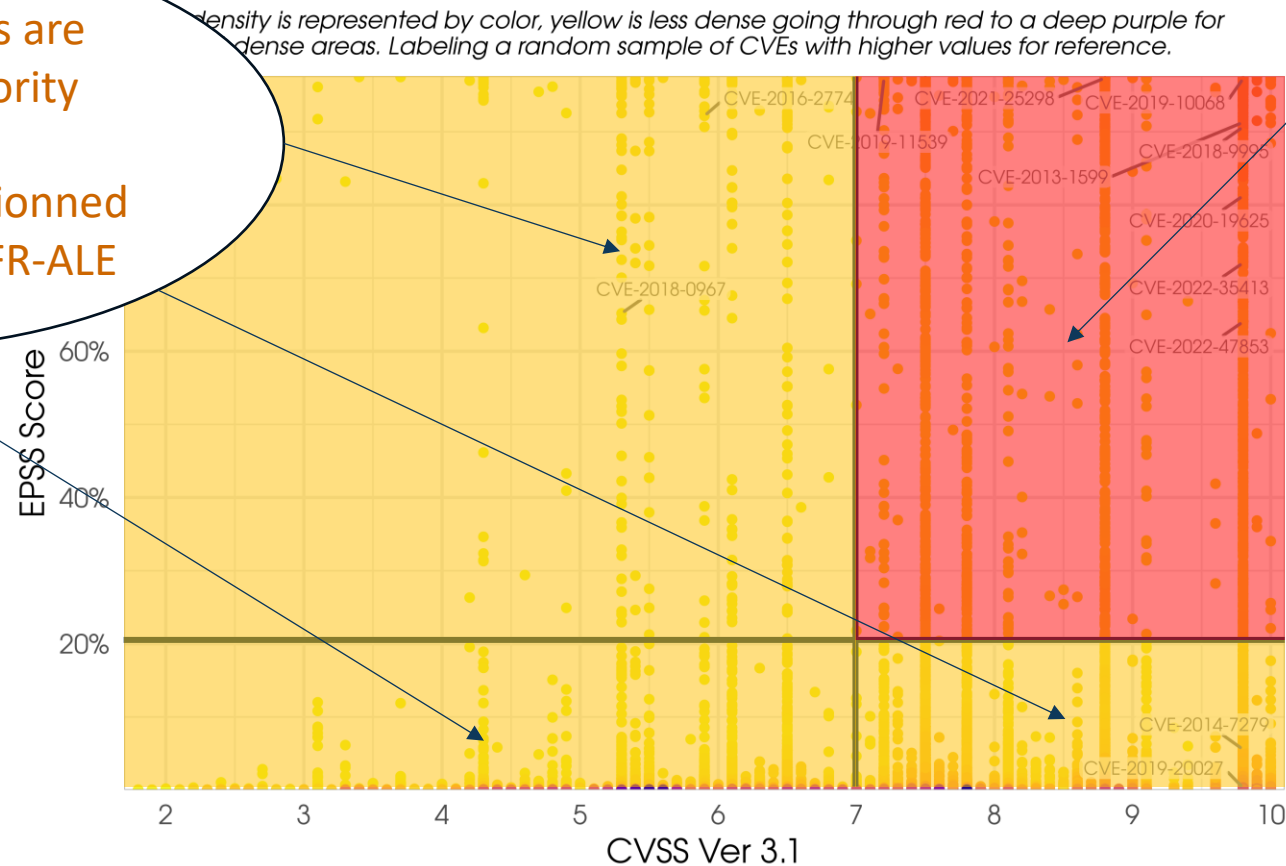
There is no « one fits all » magical method

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 mentioned by CISA KEV or CERTFR-ALE

EPSS score compared to CVSS Base Score (NVD)



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

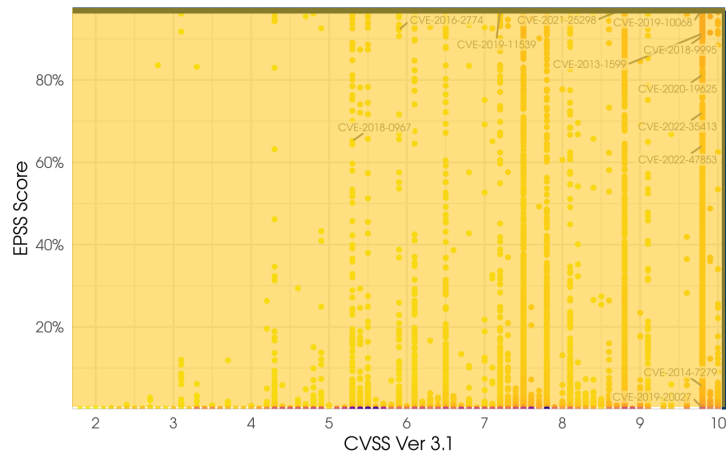
Source: https://first.org/epss/data_stats, 2024-02-28

Our recommendation: make the thresholds fit your environments

Non critical assets

EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.

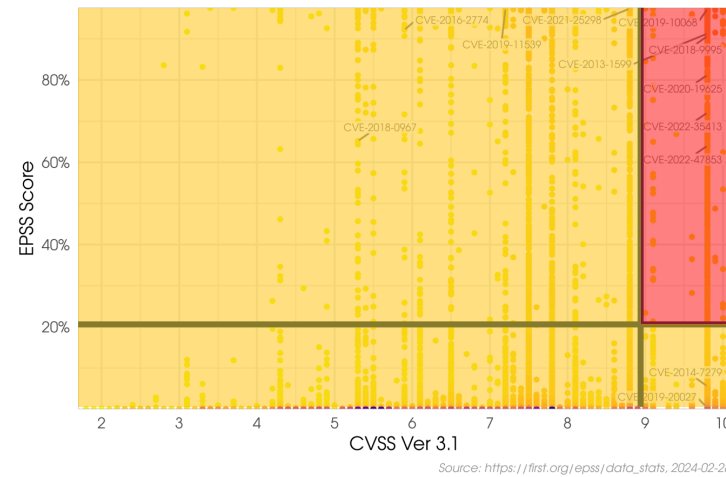


CVSS > 10
EPSS > 100%
+ CERT-FR ALE / CISA KEV

Other assets

EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.

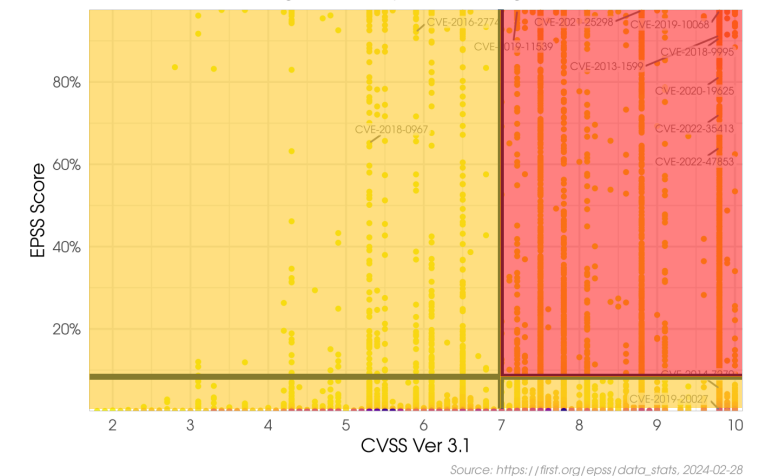


CVSS > 9
EPSS > 20%
+ CERT-FR ALE / CISA KEV

Critical assets

EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.



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)

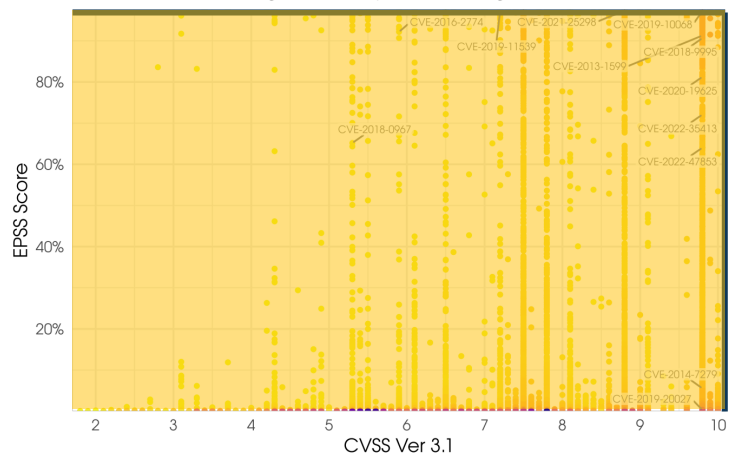
...and is already available in Cyberwatch Vulnerability Manager 😊

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

Implement this on all your devices

EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.



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

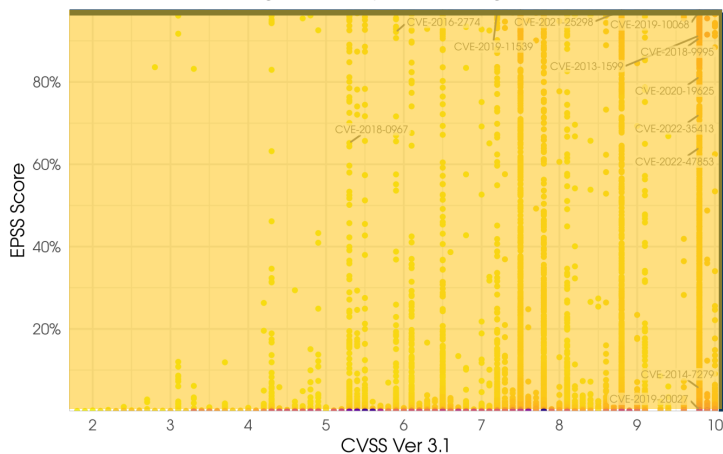
*Here, CVEs will be marked as high priority
only if they have been cherry-picked by
CERT-FR ALE*

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

Implement this on all your devices

EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.



Source: https://first.org/epss/data_stats, 2024-02-28

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**



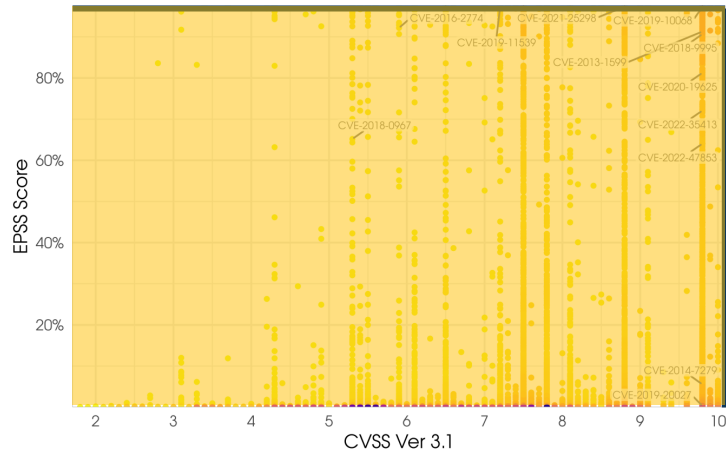
Update Windows asap
Other patches can wait

Then, when you are ready to go further...

Implement this on all your devices

EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.



Source: https://first.org/epss/data_stats, 2024-02-28

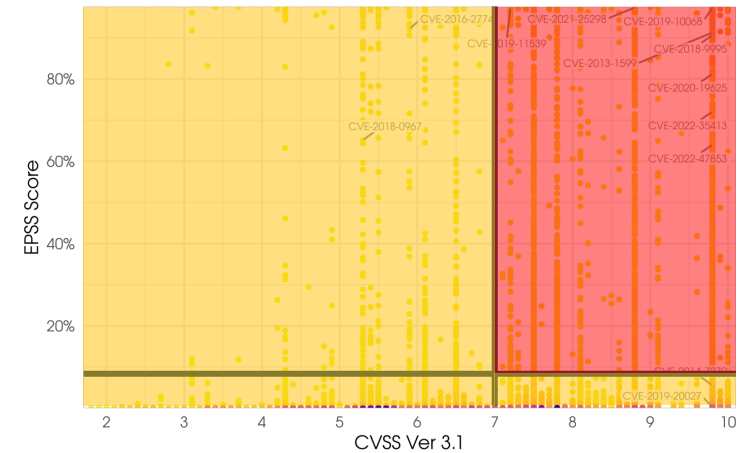
CVSS > 10
EPSS > 100%
+ CERT-FR ALE

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

Critical assets

EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.



Source: https://first.org/epss/data_stats, 2024-02-28

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



H E X A T R U S T
CLOUD CONFIDENCE & CYBERSECURITY

