SYRN

OSSIR

Juin 2026

La mort du CVSS : Changez votre vision de la Veille CVE

THREAT INTELLIGENCE · VULNERABILITY MANAGEMENT

QUI EST-CE ?

Bastien CACACE

Fondateur de SYRN

+12 annés d’expérience en CyberSécurité Offensive (XMCO)

Auteur de la newsletter “Erreur 403”

Alumni ESIEA MSSIS

Yannick HAMON

Co-Fondateur de SYRN

+20 années d’expérience en CyberSécurité, Ex-Associé (XMCO)

Alumni ESIEA MSSIS

...DES ANNÉES DE VEILLE “A LA MAIN”

LE PLAN

Le constat

Panorama de l’existant

Nos idées

Pour aller plus loin

PARTIE 01

LE CONSTAT

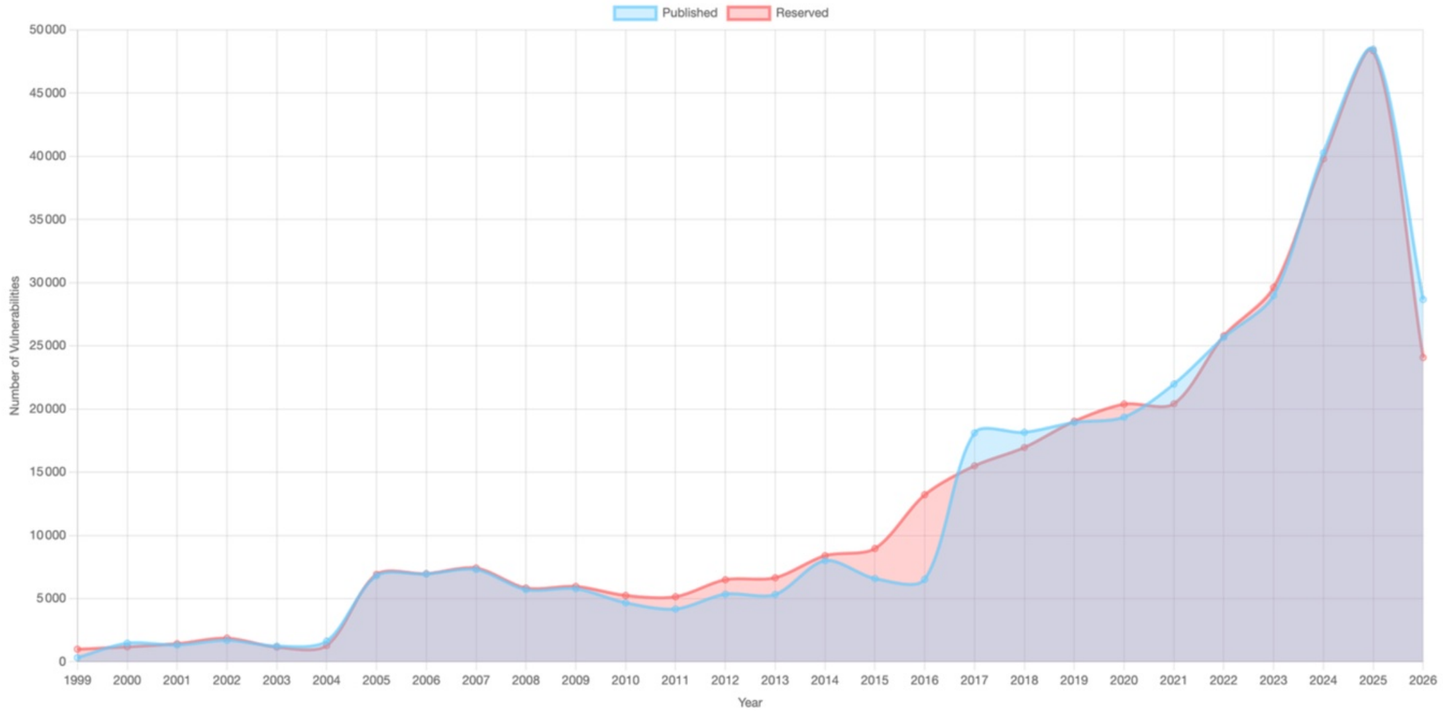
LE CONSTAT

~49 000 CVE PUBLIÉES EN 2025.

En 2026, déjà ~29 000 CVE en 5 mois...

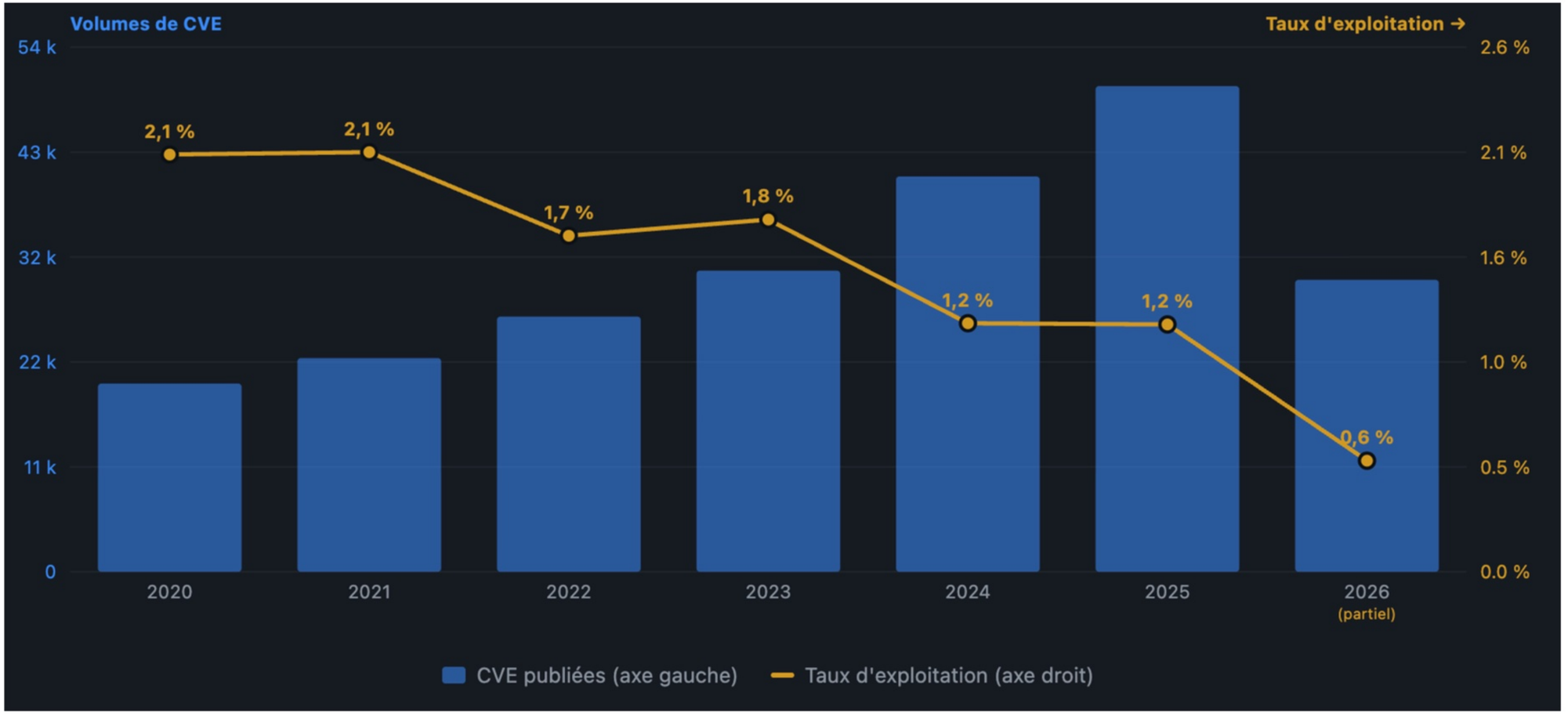
Le problème n'est plus le suivi.

C’est de prioriser.



Source : https://db.gcve.eu/stats/

LE CONSTAT

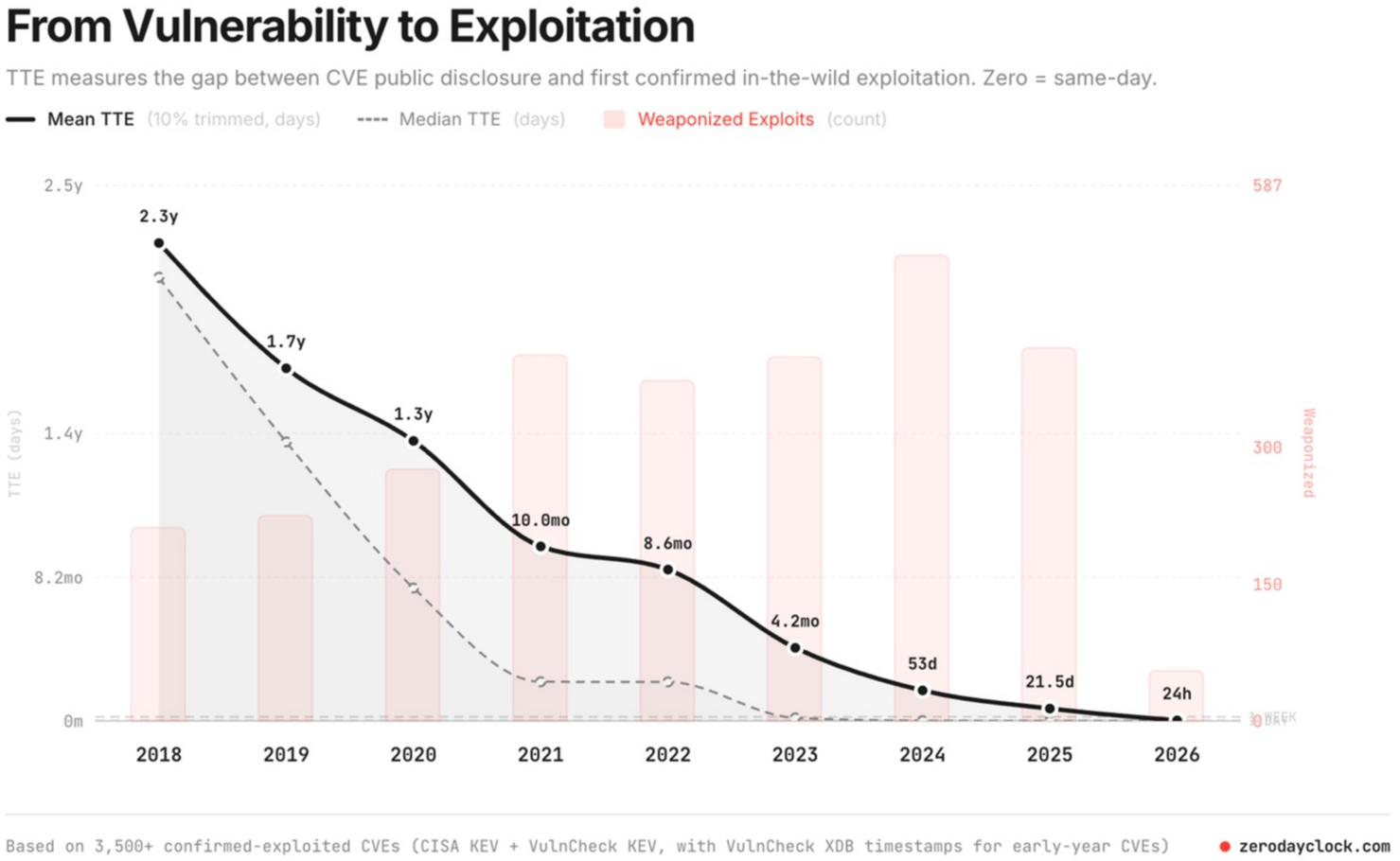


Sources

- CISA KEV
- EUKEV
- Flux MISP
- CERT-FR
- CIRCL
- Shadowserver
- HKCERT
- NCSC-NL

Moins de 1% des CVE sont réellement critiques et nécessitent une **action en urgence** sur vos équipements IT.

LE CONSTAT



Source : https://zerodayclock.com/

Le temps moyen de remédiation (MTTR) devient de plus en plus critique

PARTIE 02

PANORAMA DE L'EXISTANT

VEILLE CVE - A L'ANCIENNE (CVSS Only)

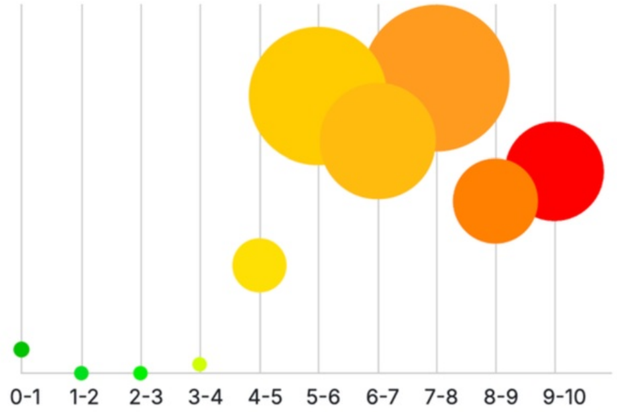
CVSS Scores Between 2025-01-01 and 2025-12-31

CVSS score distribution for CVEs published between 2025-01-01 and 2025-12-31

Period 01/01/2025 31/12/2025 Group By Year Submit

CVSS Score Range	Vulnerabilities
0-1	1217
1-2	38
2-3	309
3-4	667
4-5	3913
5-6	9961
6-7	8337
7-8	10596
8-9	6176
9+	7234
Total	48448

Weighted Average CVSS Score: 7.3



CVSS > 7.0

+24K CVE

(49,55%).

Source : https://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=&startdate=2025-01-01&enddate=2025-12-31

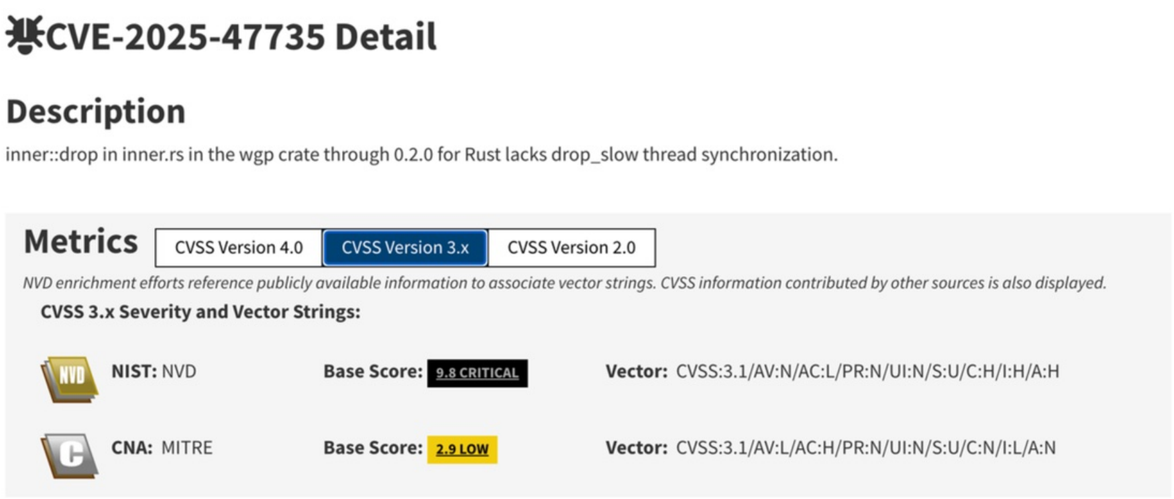
VEILLE CVE - A L'ANCIENNE (CVSS Only)

Source : https://app.syrn.fr/overview

Chaque jour, plusieurs dizaines de CVE critiques (CVSS >= 9)

VEILLE CVE - A L'ANCIENNE (CVSS Only)

Divergences des sources...



CVE-2025-47735 Detail

Description

inner::drop in inner.rs in the wgp crate through 0.2.0 for Rust lacks drop_slow thread synchronization.

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:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CNA: MITRE **Base Score:** 2.9 LOW **Vector:** CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

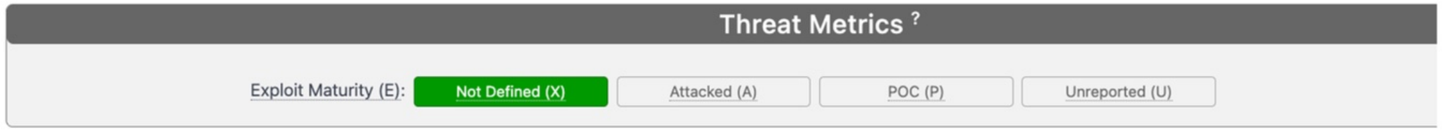
Source : https://nvd.nist.gov/vuln/detail/CVE-2025-47735

#	CVE ID	NVD SCORE	GITHUB SCORE	DRIFT
1	CVE-2026-40898 FLIP	7.5 High	5.3 Medium	Δ 2.2
2	CVE-2026-33245 FLIP	4.7 Medium	8 High	Δ 3.3
3	CVE-2026-47759 FLIP	5.4 Medium	8.7 High	Δ 3.3
4	CVE-2026-47760 FLIP	5.4 Medium	8.7 High	Δ 3.3
5	CVE-2026-47761 FLIP	5.4 Medium	8.7 High	Δ 3.3
6	CVE-2026-47762 FLIP	5.4 Medium	8.7 High	Δ 3.3
7	CVE-2026-44323	6.5	4.3	Δ 2.2

Source : https://rogolabs.github.io/consensus-engine/data.html

Score CVSS - Lequel choisir ? NIST NVD | CNA (MITRE, GITHUB, VulDB...)

VEILLE CVE-NG : CVSSv4 A LA RESCOUSSE ?



Introduit des métriques **Threat (Exploit Maturity).**

Un vrai progrès conceptuel mais :

~34 % seulement des **CVE 2026** portent un score v4 à ce jour.

Et les métriques Threat sont rarement mises à jour…

VEILLE CVE-NG : CVSSv4 A LA RESCOUSSE ?

Limitations :

- **+ de métriques** (de 22 à 32)
- **Microsoft, Red Hat, Oracle** sont toujours en **v3.1**
- Introduction de **plusieurs nomenclatures** compléxifiant la compréhension pour les néophytes :
    - **CVSS-B** : Score Base uniquement
    - **CVSS-BT** : Score Base + Threat.
    - **CVSS-BE** : Score Base + Environmental.
    - **CVSS-BTE** : Score Base + Threat + Environmental.

Source : https://www.first.org/cvss/calculator/4.0

VEILLE CVE 2.0 : CVSS x EPSS

v5 le 15 juin 2026

EPSS
Exploit Prediction Scoring System

Prédit la probabilité d'exploitation à 30 jours

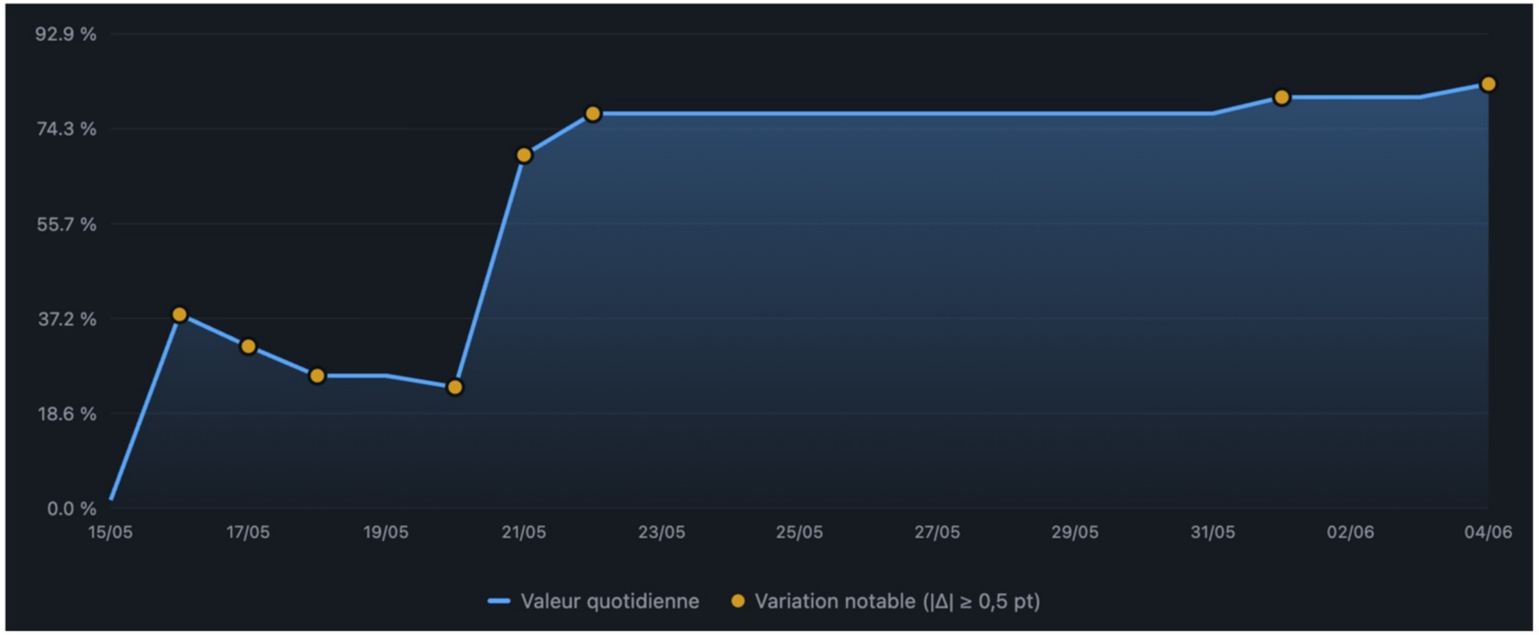
Limitations :

- **Boîte noire** : Peu d'informations sur le modèle de variation du score
- **Biais structurel** : Télémétrie nord-américaine, surface Internet ouverte.
- **Mise à jour lente** du score décalée avec la réalité (1 fois / jour)

Source : https://www.first.org/epss/model

VEILLE CVE 2.0 : CVSS x EPSS - Exemple CISCO SD-WAN

CVE-2026-20182 / 14-05-2026 / CVSS 10



Evolution du score EPSS (First)

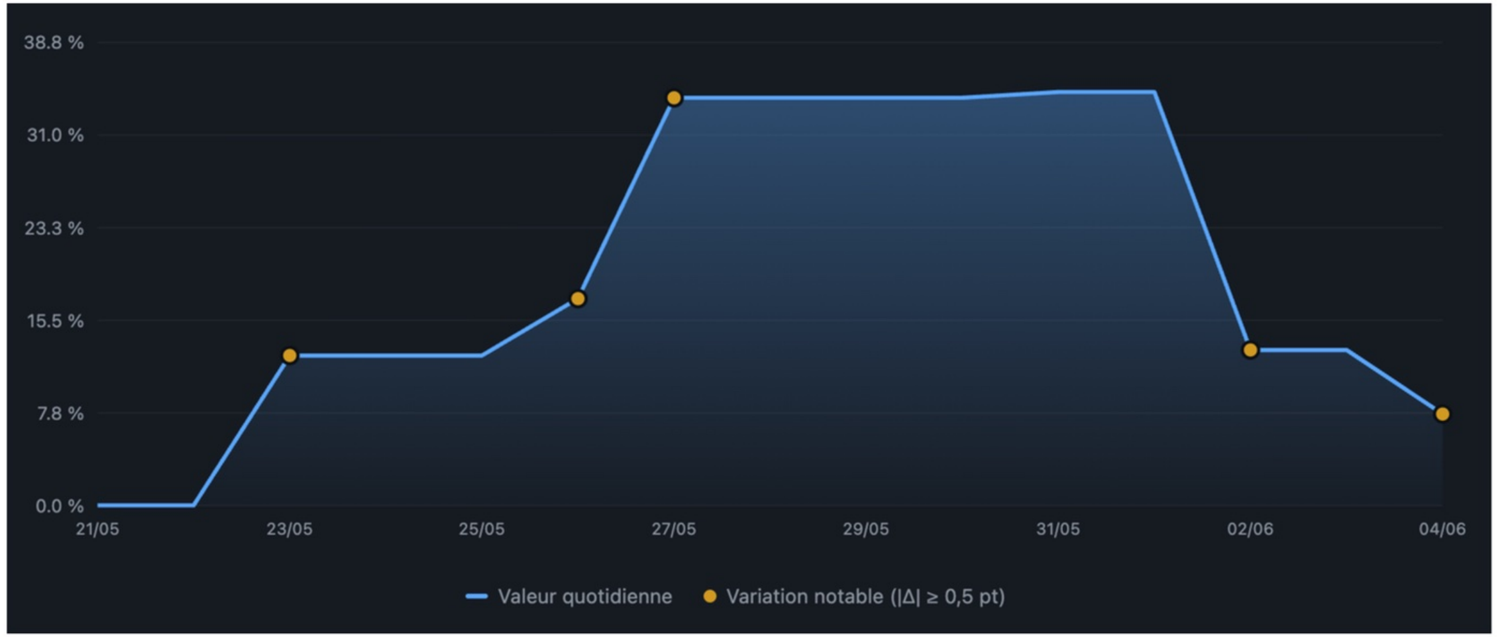
Score MAX: <85%

Score Actuel: 83.125 %

- Mise à disposition d'un module MetaSploit le 14 mai
- **À J+1 : EPSS à 1,56 %** pour une RCE CVSS 10.0 déjà au **KEV** le 14 mai
- Classée comme automatisable avec impact totale (SSVC)

VEILLE CVE 2.0 : CVSS x EPSS - Exemple DRUPAL

CVE-2026-9082 / 20-05-2026 / CVSS 9.8



Evolution du score EPSS (First)

Score MAX: <35%

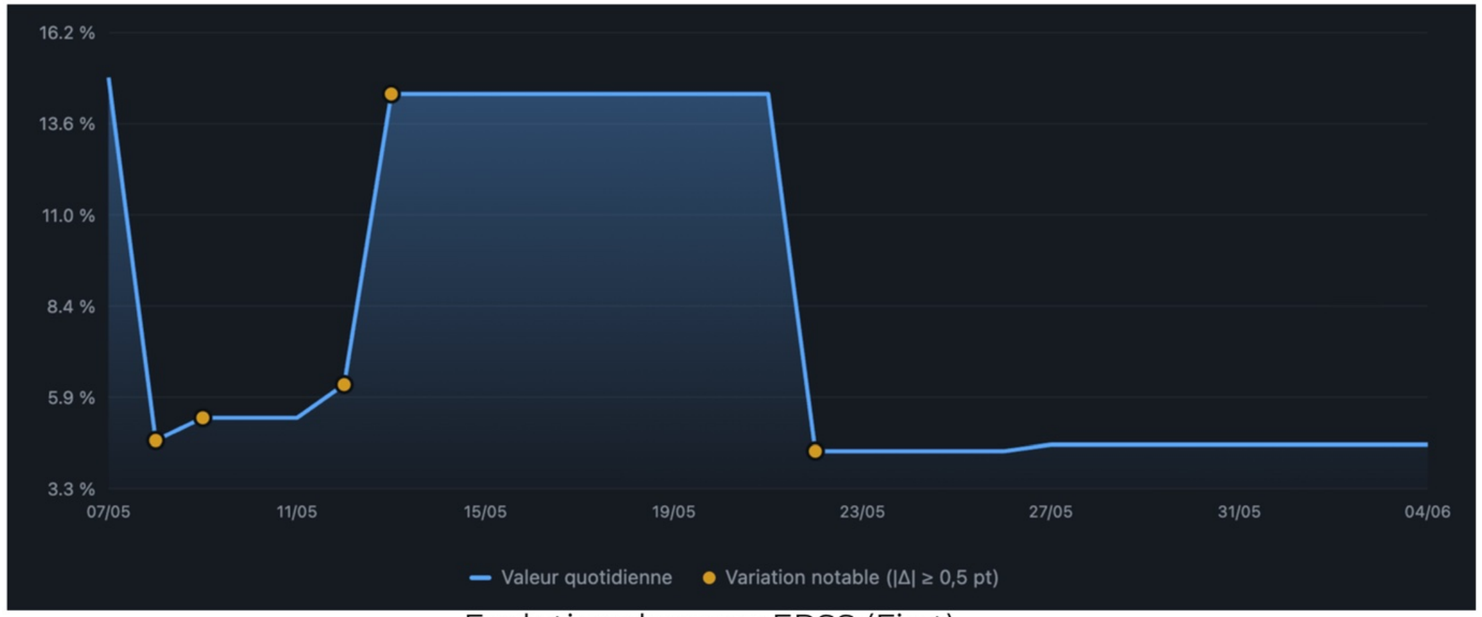
Score Actuel: 13.033 %

Pourtant :

- Mise à disposition d'un PoC sur GitHub le 21 mai
- Ajouté le **22 mai au CISA KEV - exploitée**
- Classée comme automatisable avec impact totale (SSVC)

VEILLE CVE 2.0 : CVSS x EPSS - Exemple PALO ALTO Pan-Os

CVE-2026-0300 / 06-05-2026 / CVSS 9.8



Evolution du score EPSS (First)

Score MAX: <15%

Score Actuel: 4,536 %

Pourtant :

- Ajouté le **6 mai 2026 au CISA KEV - exploitée**
- Mise à disposition d'un PoC sur GitHub
- Classée comme automatisable avec impact totale (SSVC)

PARTIE 03

NOS IDEES

NOS REFLEXIONS :

Enjeu : Réduire le MTTR (enfin quand cela est **réellement nécessaire**)

Les piliers fondamentaux :

- **La CTI au service de la CVE :** aggréger & **enrichir** les CVE avec **toutes** les informations disponibles (techniques ou non)
- **Qualification Automatique** | Temps-réel | 24/7
- **Score UNIQUE & UNIVERSEL** permettant une surcouche de personnalisation (**Self-Risk based** : exposition Internet, obligations réglementaires, sensibilité)

NOS REFLEXIONS :

Sources officielles

Réseaux sociaux / Fil de discussions

PoC et Exploits

Métriques CVSS / EPSS / SSVC
Exploits / PoC / framework offensifs
Ransomware / APT
CWE
Alertes CERT-FR / KEV
Activités sur les réseaux

METHODE DE CALCUL DU SCORE

	Note Maximale	CVEs 2025
• **Exploitation Active** (KEV, Shadow Server, Bug Bounty…)	40	1.2%
• **Kits d'exploitation** (PoC Github, MetaSploit, Nuclei, …)	38	22%
• Score **CVSS**	35	
• **Réseaux sociaux / Fil de discussions**	25	8.4% >= 5 mentions
• **Vélocité** (CVE < 3 jours)	25	0.2%
• Score **EPSS**	20	
• **Informations tierces** (Ransomware, APT, CWE, SSVC, CERT-FR…)	15	0.3% Ransomware Alerte CERT FR

5.4 % >= 60 et 1.6% >= 80

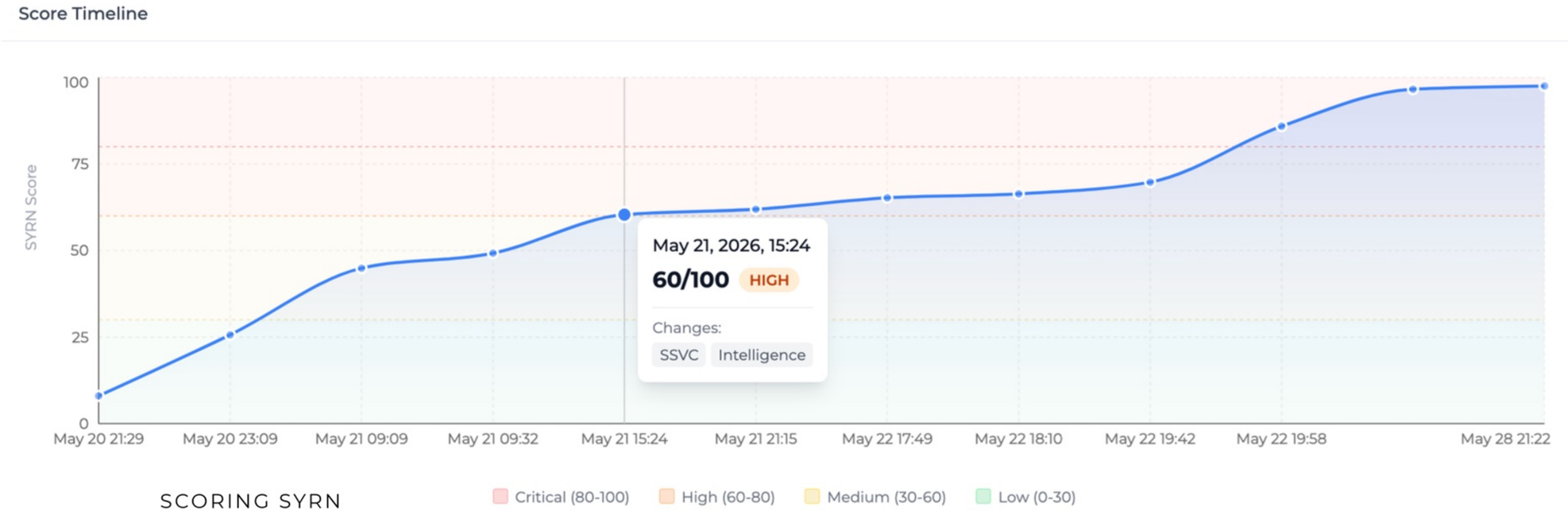
SCORING UNIQUE - Exemple DRUPAL

CVE-2026-9082 / 20-05-2026 / CVSS 9.8

TIMELINE EPSS

Score EPSS MAX: <35% (au bout d'une semaine)

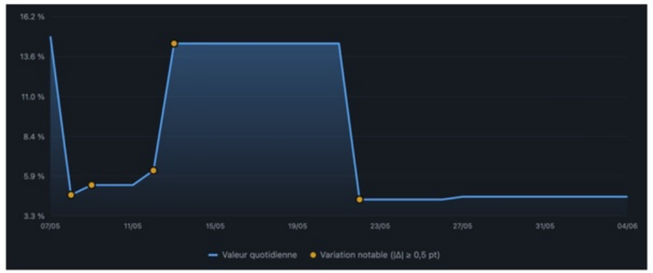
Score EPSS Actuel: 13.033 %



SCORING SYRN

SCORING UNIQUE - Exemple PALO ALTO PAN OS

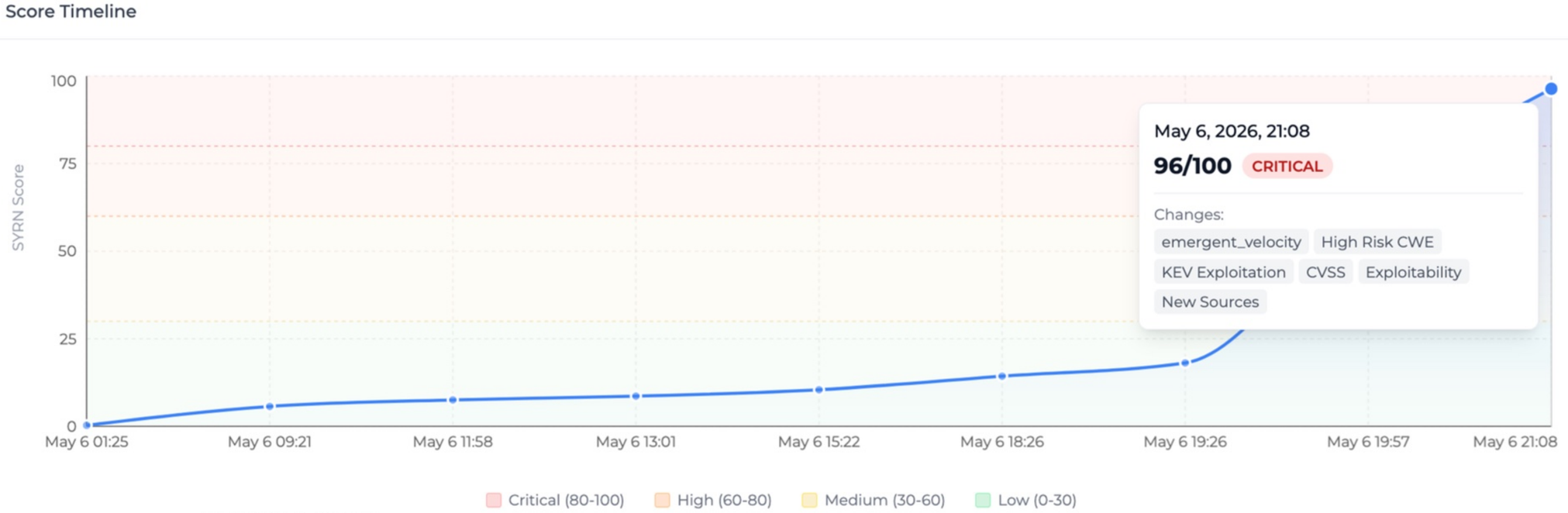
CVE-2026-0300 / 06-05-2026 / CVSS 9.8



Score EPSS MAX: <15%

Score EPSS Actuel: 4,536 %

TIMELINE EPSS



SCORING SYRN

PARTIE 04

OSSIR

ET DEMAIN ?

SYRN

Minority Report x IA

Corréler les signaux faibles sans CVE :

- Conférences, articles de presse, réseaux sociaux
- Analyse de sources non occidentales
- PoC sans aucune information
- Publication d'éditeurs (i.e. security update) sans information (ni CVE, ni CVSS…)

Favoriser une **approche communautaire :**

- Intégrer des Retex terrain pour enrichir la CVE
- Partager sur les méthodes de détection/remédiation
- Validation technique des PoC (ou par IA)

SYRN

Q & A

EMAIL
contact@syrn.fr

WEB
syrn.fr · app.syrn.fr

LINKEDIN
/company/syrn-security