

GUIDE

Score de risque cyber : CVSS, EPSS & KEV pour prioriser

Comprendre ce que mesure chaque score, ce qu'aucun ne dit seul, et comment les combiner pour corriger d'abord ce qui vous expose vraiment.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~11 min Édition 2026 sedona-ai.com

Face à des dizaines de vulnérabilités, la bonne question n'est pas « laquelle est la plus grave ? » mais « laquelle risque de me coûter cher, maintenant ? ». Trois signaux y répondent : CVSS mesure la sévérité technique, EPSS estime la probabilité d'exploitation, et le catalogue KEV de la CISA liste ce qui est activement exploité. Aucun ne suffit seul. Ce guide vous montre comment les recouper pour prioriser vos correctifs sans vous noyer.

À retenir

- CVSS mesure une sévérité technique potentielle (0 à 10), pas un risque réel : un score « critique » ne veut pas dire que la faille sera exploitée.
- EPSS estime, par machine learning, la probabilité qu'une CVE soit exploitée dans les 30 jours à venir (score de 0 à 1, recalculé chaque jour).
- Le catalogue CISA KEV est un constat rétrospectif : il ne liste que les vulnérabilités dont l'exploitation active est prouvée — action immédiate.
- L'exploitation réelle est rare : environ 2,5 à 3 % des CVE publiées connaissent une activité d'exploitation sur 30 jours ; prioriser sur CVSS seul gaspille vos ressources.
- La bonne méthode recoupe les trois signaux, du plus urgent au plus indicatif : KEV, puis EPSS élevé, puis CVSS pondéré par le contexte d'exposition réel.
- La directive BOD 22-01 de la CISA n'oblige que les agences fédérales américaines ; pour une PME/ETI française, traiter les failles KEV en priorité reste une excellente pratique volontaire.

01 Le problème : trop de failles, pas assez de temps

Le volume de vulnérabilités publiées explose : l'année 2024 a établi un record historique, avec 40 704 CVE recensées selon le FIRST.org — en forte hausse par rapport à 2023. Aucune équipe, aucun budget ne permet de tout corriger en même temps. La priorisation n'est donc pas un luxe : c'est la seule stratégie viable.

40 704

CVE publiées en 2024, record historique (en forte hausse vs 2023)

FIRST.org — The 2024 Vulnerability Forecast: Year in Review, 2025

CVE, c'est quoi ?

Une CVE (Common Vulnerabilities and Exposures) est l'identifiant public unique attribué à une vulnérabilité connue, du type CVE-2024-XXXXX. C'est le langage commun de tout l'écosystème sécurité.

02 CVSS : la sévérité technique, pas le risque

CVSS (Common Vulnerability Scoring System, géré par le FIRST.org) attribue à chaque vulnérabilité un score de 0 à 10 reflétant sa gravité technique intrinsèque, traduit en note qualitative : faible, moyen, élevé, critique. C'est utile pour comparer des failles entre elles — mais c'est tout ce que ça dit.

Le piège du « critique »

Un score CVSS de 9,0-10,0 mesure un potentiel de dégâts, pas une probabilité d'attaque. Il ne tient compte ni de votre exposition sur Internet, ni de la criticité de l'actif, ni de l'existence d'un exploit. Prioriser sur le seul CVSS, c'est risquer de traiter des failles qui ne seront jamais exploitées.

Détail qui compte dans un rapport : CVSS v4.0 est la version actuelle du standard (publiée en novembre 2023), mais CVSS v3.1 reste très largement utilisé par les scanners et les CERT. Précisez toujours la version du score que vous citez.

03 EPSS : la probabilité d'exploitation

EPSS (Exploit Prediction Scoring System, également FIRST.org) répond à la question que CVSS ignore : quelle est la probabilité que cette faille soit exploitée dans les 30 prochains jours ? C'est un modèle de machine learning, recalculé chaque jour à partir de signaux observés (exploits publics, scans, mentions dans des frameworks d'attaque...), et non un jugement d'expert. Le score va de 0 à 1, accompagné d'un percentile de classement.

2,5–3 %

des CVE publiées connaissent une exploitation observée sur 30 jours
FIRST.org — EPSS FAQ, 2025

Ce chiffre est la clé de toute la démarche : la très grande majorité des vulnérabilités ne sont jamais exploitées. C'est pourquoi la distribution des scores EPSS est massivement concentrée près de zéro — et pourquoi un EPSS élevé est un signal fort et rare qui mérite votre attention.

04 KEV : l'exploitation confirmée, ici et maintenant

Le catalogue KEV (Known Exploited Vulnerabilities) de la CISA américaine n'est pas prédictif comme EPSS : c'est un constat rétrospectif. Une CVE n'y entre que si son exploitation active dans la nature est prouvée. Si une de vos failles y figure, le débat est clos — elle est attaquée en ce moment même.

1. Un identifiant CVE attribué à la vulnérabilité.
2. Une preuve fiable d'exploitation active dans la nature.
3. L'existence d'une consigne de remédiation claire (correctif ou contournement).

≈ 0,5 %

des CVE publiées figurent au catalogue CISA KEV
FIRST.org — EPSS FAQ, 2025

BOD 22-01 : obligatoire pour qui ?

La directive BOD 22-01 (CISA, nov. 2021) impose des délais de remédiation fixes sur les failles KEV — mais uniquement aux agences fédérales civiles américaines. Pour une PME/ETI française, ce n'est pas une obligation légale : c'est une excellente pratique volontaire que la CISA recommande à toute organisation.

05 Pourquoi aucun score ne suffit seul

Chacun de ces trois signaux répond à une question différente. Les confondre — ou n'en utiliser qu'un — conduit soit à corriger des failles inoffensives, soit à ignorer une porte grande ouverte. Le tableau ci-dessous les remet à leur place.

Signal	Ce qu'il mesure	Nature	Rôle dans la priorisation
CVSS	Sévérité technique intrinsèque (0-10)	Note fixe, indépendante du contexte	Pondérer par l'exposition réelle — jamais utiliser seul
EPSS	Probabilité d'exploitation sous 30 jours (0-1)	Prédictif, recalculé chaque jour	Détecter les failles à risque avant même toute attaque
KEV	Exploitation active prouvée	Constat rétrospectif, binaire	Déclencher une action immédiate, sans discussion

06 La méthode : recouper les trois signaux

La priorisation efficace enchaîne les trois signaux, du plus urgent au plus indicatif. À chaque niveau, vous filtrez le bruit et vous concentrez vos ressources là où le risque est réel.

1. La faille est-elle dans le catalogue KEV ?

Si oui : exploitation active confirmée. Remédiation immédiate, en tête de liste, quel que soit son score CVSS.

2. Son score EPSS est-il élevé (percentile haut) ?

Forte probabilité d'exploitation prochaine, même sans preuve KEV encore publiée. À traiter en urgence rapprochée.

3. CVSS élevé + actif réellement exposé ?

Un CVSS fort ne compte que pondéré par le contexte : l'actif est-il accessible depuis Internet, héberge-t-il des données sensibles, existe-t-il un contrôle compensatoire ? Ce signal se traite après les deux premiers, jamais seul.

En clair

KEV = « on m'attaque, je corrige tout de suite ». EPSS élevé = « je vais être attaqué, je corrige vite ». CVSS élevé + actif exposé = « ce serait grave si on m'attaquait, je planifie ».

07 Où Sedona Radar intervient

Recouper CVSS, EPSS et KEV à la main, sur des dizaines de vulnérabilités et à chaque nouveau scan, est ingérable pour une équipe IT de PME. Sedona Radar analyse ce que votre domaine expose sur Internet (ce qui est visible depuis Internet), détecte les vulnérabilités et les classe par gravité, avec des conseils de correction. Vous obtenez une liste d'actions ordonnée, pas un catalogue de scores bruts.

Radar évalue, il ne certifie pas

Sedona Radar donne des indicateurs de maturité sur plusieurs référentiels (dont NIS2 et l'Hygiène ANSSI). C'est une évaluation, pas une certification : il n'existe aucune certification NIS2. Données stockées dans l'Union européenne.

§ Sources

1. FIRST.org — CVSS (Common Vulnerability Scoring System), versions et documentation officielle — <https://www.first.org/cvss/>
2. FIRST.org — EPSS (Exploit Prediction Scoring System), présentation officielle — <https://www.first.org/epss/>
3. FIRST.org — EPSS FAQ (statistiques d'exploitation et proportion KEV) — <https://www.first.org/epss/faq>
4. FIRST.org — The 2024 Vulnerability Forecast: Year in Review (statistiques CVE 2024) — <https://www.first.org/blog/20250106-Vulnerability-Forecast-Year-in-Review>
5. CISA — Known Exploited Vulnerabilities Catalog — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
6. CISA — BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities — <https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities>
7. NVD (NIST) — Dashboard officiel des statistiques CVE — <https://nvd.nist.gov/general/nvd-dashboard>

Découvrez ce qui vous expose vraiment

Sedona Radar analyse ce que votre domaine expose sur Internet et classe les vulnérabilités détectées par gravité. Lancez un premier scan gratuit, sans engagement.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit