# Comparatif entre la CVSS v4 et CVSS v3.1

Dans mes rapports vous y constaterez une différence, celle de la CVSS de mon rapport AD et Wifi, et celle de mon rapport Web et Linux. En effet, durant la réalisation du pentest début d’année, il était question de travailler avec la CVSS 3.1 mais quelques mois plus tard, j’apprends la sortie de la nouvelle génération de la norme Common Vulnerability Scoring System.

## Les améliorations qui ont été apporté :

1. Elle vise à rendre la notation plus simple et plus claire en éliminant toute ambiguïté. Elle propose des conseils et des définitions plus précises pour les métriques, notamment en affinant les concepts de « Complexité de l’attaque » et « Exigences de l’attaque ». Ces ajustements ont pour objectif de rendre le processus de notation plus accessible, contribuant à une évaluation plus précise des vulnérabilités tout en assurant une uniformité entre les différentes organisations.
2. Renforcement de l’adaptabilité : Le CVSS v4.0 introduit de nouveaux indicateurs et une structure modulaire, permettant aux organisations de personnaliser la notation en fonction de leurs besoins. Elle permet de prendre en compte la technologie opérationnelle, différencie les interactions utilisateur actives et passives, facilitant une évaluation détaillée de la vulnérabilité dans divers contextes.
3. Améliore la prise en compte du risque en incluant la probabilité d'exploitation et les conséquences potentielles d'une attaque. Il intègre des informations sur les menaces et l'environnement dans la notation, offrant ainsi une évaluation des risques plus réaliste. De nouveaux concepts comme « Automatable », « Récupération » et « Effort d'atténuation » ajoutent des nuances à la compréhension de chaque vulnérabilité.

## Comparatif entre deux calculateurs :

D’après un comparatif en ligne basé sur les deux calculateurs CVSS V3 Calculator et CVSS V4 Calculator, on peut analyser une vulnérabilité avec les vecteurs suivants :

[CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N](https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

Concernant la CVSS 4.0, cela donnerait 5.4 -> Medium

Comparons ce qui est comparable, il ne faut pas définir plusieurs paramètres, on compare le basique au basique !

Un vecteur avec les paramètres [AV:A/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H&version=3.1)

Dans cvss 3, cela donnerait un 7,4 -> élevé

## Conclusion :

CVSS 4, actuellement en version préliminaire, représente une avancée par rapport à CVSS v3.1. Cependant, des ajustements ultérieurs sont possibles, comme cela a été le cas lors de la transition de CVSS 2 à 3. Le processus de mise en œuvre est généralement lent. Pour le moment, l'impact sur la sécurité des applications reste peu clair, car le CVSS semble principalement axé sur l'infrastructure et les vulnérabilités de type OT. Les aspects tels que la localisation et le contexte commercial sont encore peu pris en compte dans les scores de la CIA. Néanmoins, une amélioration notable réside dans la flexibilité et la modifiabilité des scores.

Source : <https://www.first.org/cvss/v4-0/>

Source : <https://phoenix.security/cvss-v4-whats-new-and-how-does-it-differ-from-cvss-v3-1/>