

# OpenVAS

Informações sobre o funcionamento e arquitetura do OpenVAS - Open source Vulnerability Assessment Scanner.

- Classificação CVSS de vulnerabilidade

# Classificação CVSS de vulnerabilidade

No contexto de segurança digital, o ranqueamento *Common Vulnerability Scoring System* (CVSS), atualmente em sua 3ª iteração, se apresenta como uma métrica bastante útil para classificar vulnerabilidades em serviços e sistemas distribuídos de acordo com alguns critérios de diferentes pesos. A elaboração da pontuação CVSS surgiu como uma necessidade de distinguir vulnerabilidades de acordo com sua gravidade, afinal de contas, com a evolução e disseminação de equipamentos permeados por conexões de Internet (a "Internet das coisas"), tornou-se cada vez mais identificar pontos de grande vulnerabilidade suscetíveis a ataques nos diversos sistemas e serviços oferecidos atualmente.

A pontuação CVSS é, então, bastante utilizada em contextos empresariais para classificar falhas de segurança que podem vir a comprometer usuários e/ou serviços. O método de cálculo da pontuação CVSS é de acesso público, e muitos programas de escaneamento de vulnerabilidade, como o OpenVAS, o utilizam amplamente em varreduras automatizadas.

## Cálculo da métrica

Dessa forma, vamos explorar um pouco cada critério utilizado no cálculo da pontuação CVSS para compreender melhor sua grande aplicabilidade nos mais diversos contextos.

Os valores analisados no cálculo da pontuação são os valores **base**, **temporal** e **ambiental**.

### Base

A métrica do valor base se pauta nos aspectos mais simples de uma vulnerabilidade, aqueles que independem do tempo decorrido e do contexto em que essa vulnerabilidade está inserida. Este valor tem subcritérios definidos no seu cálculo:

- **Vetor de Acesso:** este primeiro subcritério diz respeito a quão fácil é a exploração da vulnerabilidade em termos de proximidade do sistema. Uma vulnerabilidade que só possa

ser explorada mediante à presença física do atacante é considerada de baixo risco vetor de acesso, por exemplo;

- **Complexidade de Acesso:** este subcritério diz respeito a quantidade de pré-requisitos que fogem do controle do invasor para que seu ataque seja possível, como alguma informação adicional sobre o sistema alvo que não possa ser obtida normalmente;
- **Privilégios Exigidos (PE):** este subcritério representa a quantidade de permissões (desde usuário comum até administrador) que o invasor precisa para conseguir atacar o sistema.

## Temporal

A métrica do valor temporal é elaborada de acordo com fatores que mudam ao longo do tempo e que podem agravar ou não uma falha de segurança, ou até mesmo o reconhecimento sua existência. Assim, o valor temporal está fortemente relacionado com o "nível de amadurecimento" de uma vulnerabilidade, isto é, por quanto tempo ela esteve disponível e quando foi documentada, o surgimento de atualizações e patches que eliminem a vulnerabilidade, e também o desenvolvimento de exploits para ela.

Este valor tem os seguintes subcritérios definidos no seu cálculo: maturidade dos exploits para esta vulnerabilidade e sua disponibilidade, nível de remediação até o momento, isto é, se há uma solução conhecida ou não para o problema, e confiança no relatório, com que certeza se sabe que se trata de uma vulnerabilidade, de fato.

## Ambiental

Por fim, a métrica ambiental avalia características individuais do ambiente no qual a vulnerabilidade se apresenta, portanto a mesma vulnerabilidade pode se tornar mais ou menos grave dependendo de seu contexto. Este valor é definido levando em conta, dentre outros fatores, a importância do serviço afetado para os demais (nesse caso, uma vulnerabilidade num ponto muito importante de um grande sistema deveria ser tratada com urgência), a magnitude do dano colateral possível e a utilidade do sistema invadido para o invasor.

## Classificação pela pontuação CVSS

Assim, de acordo com a pontuação CVSS calculada com base nos três parâmetros descritos acima, define-se um ranqueamento de vulnerabilidades da seguinte forma:

- 0,0 - Não apresenta risco;
- 0,1 a 3,9 - Baixo risco;
- 4,0 a 6,9 - Médio risco;
- 7,0 a 8,9 - Alto risco;
- 9,0 a 10,0 - Risco crítico;

Para mais informações sobre o cálculo da pontuação CVSS, clique [aqui](#).