**Análise da Evolução das Vulnerabilidades CWE Top 25 (2019-2024)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CWE ID** | **Vulnerabilidade** | **Descrição** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** |
| CWE-119 | Buffer Overflow | Operações de memória que podem ler ou escrever fora dos limites do buffer | 1 | 1 | 1 | 1 | 1 | 1 |
| CWE-79 | Cross-site Scripting (XSS) | Falha na validação de entrada que permite injeção de scripts maliciosos | 2 | 4 | 3 | 3 | 2 | 2 |
| CWE-89 | SQL Injection | Inserção de comandos SQL maliciosos por meio de entradas não validadas | 6 | 6 | 7 | 6 | 3 | 3 |
| CWE-200 | Information Exposure | Exposição não intencional de informações sensíveis | 4 | 3 | 5 | 4 | 4 | 4 |
| CWE-125 | Out-of-bounds Read | Leitura de dados fora dos limites do buffer pretendido | 5 | 5 | 4 | 5 | 5 | 5 |
| CWE-416 | Use After Free | Uso de memória após a sua liberação | 7 | 7 | 6 | 7 | 6 | 6 |
| CWE-78 | OS Command Injection | Injeção de comandos do sistema operativo | 11 | 11 | 13 | 11 | 7 | 7 |
| CWE-287 | Authentication Issues | Problemas na verificação de identidade | 13 | 15 | 14 | 12 | 8 | 8 |

**1. Tabela Comparativa das Principais Vulnerabilidades**

**2. Análise de Tendências**

**2.1 Vulnerabilidades Persistentes**

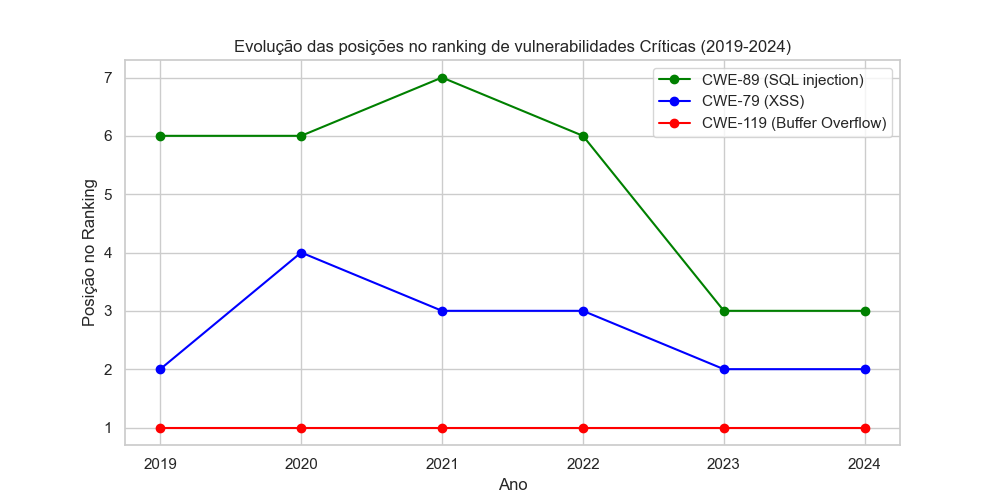
* **Buffer Overflow (CWE-119)** manteve consistentemente a primeira posição ao longo dos anos, demonstrando que problemas fundamentais de gestão de memória continuam a ser críticos.
* **Cross-site Scripting (CWE-79)** e **SQL Injection (CWE-89)** permaneceram consistentemente no top 10, indicando que vulnerabilidades relacionadas à validação de entrada continuam a ser um desafio significativo.

**2.2 Tendências Emergentes**

1. **Authentication Issues (CWE-287)** mostrou uma tendência de subida constante, movendo-se da posição 13 em 2019 para a posição 8 em 2024, refletindo a crescente importância da segurança de autenticação.
2. **OS Command Injection (CWE-78)** também demonstrou uma tendência de ascensão, especialmente nos últimos dois anos.

**2.3 Mudanças Significativas**

* Houve uma maior ênfase em vulnerabilidades relacionadas à autenticação e gestão de sessões nos últimos anos.
* Vulnerabilidades relacionadas a vazamento de informações mantiveram-se consistentemente importantes.



Assim sendo e resumindo o **CWE-119 (Buffer Overflow)** lidera consistentemente o ranking de vulnerabilidades mais perigosas entre 2019 e 2024, refletindo a complexidade de mitigar este problema em sistemas críticos. Vulnerabilidades relacionadas à validação de entradas de utilizadores, como o **CWE-79 (XSS)** e o **CWE-89 (SQL Injection)**, permanecem críticas devido à sua ampla exploração em aplicações web modernas.

A subida do **CWE-287 (Authentication Issues)** demonstra a relevância crescente de falhas de autenticação, provavelmente devido ao aumento de sistemas distribuídos e APIs. Já vulnerabilidades como o **CWE-78 (OS Command Injection)** mostram sinais de melhoria, indicando uma adoção mais ampla de práticas seguras