Modelo de Documento para Catalogação e Categorização de Vulnerabilidades em Sistemas de Computador

1. Introdução

Este documento tem como objetivo catalogar e categorizar as vulnerabilidades encontradas em sistemas de computador, abrangendo software, servidores e sistemas operacionais. A catalogação sistemática de vulnerabilidades é crucial para a implementação de medidas corretivas eficazes e para a melhoria contínua da segurança.

2. Metodologia

A metodologia de catalogação envolve a identificação, classificação e documentação detalhada das vulnerabilidades. A categorização é feita com base em critérios como tipo de vulnerabilidade, impacto, complexidade de exploração e recomendação de mitigação.

3. Estrutura do Documento

1. **Identificação da Vulnerabilidade**
    - **ID da Vulnerabilidade:** Identificador único para a vulnerabilidade.
    - **Data de Identificação:** Data em que a vulnerabilidade foi identificada.
2. **Descrição da Vulnerabilidade**
    - **Título:** Nome ou descrição curta da vulnerabilidade.
    - **Descrição Completa:** Descrição detalhada da vulnerabilidade, incluindo como ela pode ser explorada.
    - **Componente Afetado:** Especificar o software, servidor ou sistema operacional afetado.
3. **Classificação**
    - **Categoria:** (e.g., SQL Injection, Buffer Overflow, XSS, Configuração Incorreta)
    - **Impacto:** (e.g., Alta, Média, Baixa) com base na potencial gravidade da vulnerabilidade.
    - **Complexidade de Exploração:** (e.g., Alta, Média, Baixa) indicando a facilidade com que a vulnerabilidade pode ser explorada.
    - **Vetor de Ataque:** (e.g., Rede, Local, Físico)
4. **Avaliação**
    - **CVSS Score:** Pontuação de acordo com o Common Vulnerability Scoring System (CVSS).
    - **Consequências Potenciais:** Impacto potencial na confidencialidade, integridade e disponibilidade dos sistemas.
5. **Mitigação**

- **Soluções Recomendas:** Passos específicos para corrigir ou mitigar a vulnerabilidade.
- **Patches Disponíveis:** Informações sobre patches ou atualizações que abordam a vulnerabilidade.
- **Procedimentos de Hardening:** Recomendações de hardening para evitar futuras explorações.

6. **Status**
    - **Estado Atual:** (e.g., Identificado, Em processo de correção, Corrigido)
    - **Data da Correção:** Data em que a vulnerabilidade foi corrigida.
    - **Responsável:** Equipe ou indivíduo responsável pela correção.

4. Exemplo de Catalogação
ID da Vulnerabilidade: VULN-2024-001

Data de Identificação: 01/05/2024

Título: SQL Injection em Formulário de Login

Descrição Completa: Uma vulnerabilidade de SQL Injection foi encontrada no formulário de login do sistema XYZ. A vulnerabilidade permite que um atacante injete comandos SQL maliciosos, comprometendo a integridade e confidencialidade dos dados.

Componente Afetado: Sistema XYZ

Categoria: SQL Injection

Impacto: Alta

Complexidade de Exploração: Média

Vetor de Ataque: Rede

CVSS Score: 8.5

Consequências Potenciais:

- Acesso não autorizado a dados sensíveis
- Modificação ou exclusão de dados

Soluções Recomendas:

- Utilizar consultas parametrizadas para todas as interações com o banco de dados.
- Implementar validação de entrada rigorosa.

Patches Disponíveis:

- Patch 1.0.1 disponível no site do fornecedor que corrige a vulnerabilidade.

Procedimentos de Hardening:

- Realizar auditoria regular de código.

- Treinar desenvolvedores em práticas seguras de codificação.

Estado Atual: Em processo de correção

Data da Correção: N/A

Responsável: Equipe de Desenvolvimento