CERT-MZ

Tech Talk

Gestão de Vulnerabilidades

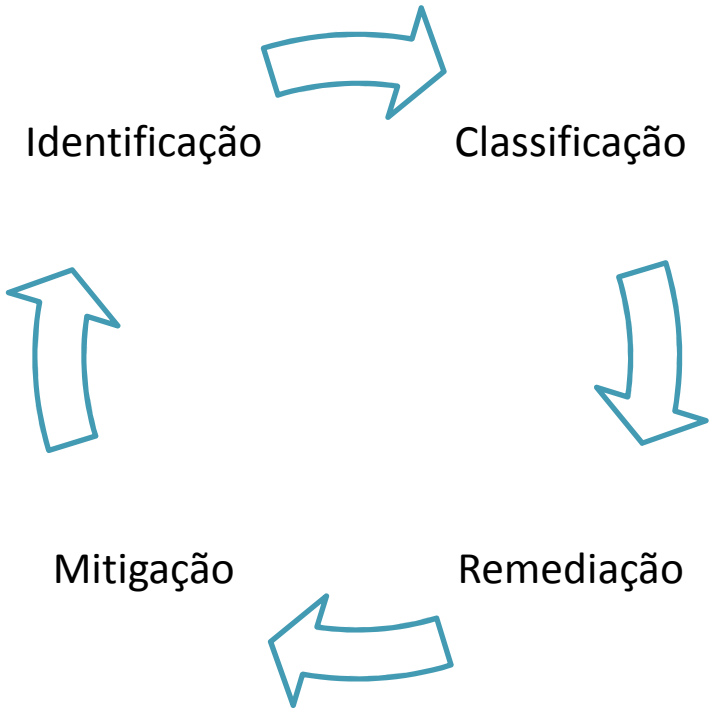
Alsone Guambe
aguambe@cert.mz

O que é vulnerabilidade?

Atributo ou característica de sistema que pode ser explorada de modo a causar um efeito adverso

Gestão de vulnerabilidades

Gestão de vulnerabilidade é o processo de se manter no topo das vulnerabilidades para que as correcções sejam frequentes e eficazes.



Tipos de vulnerabilidades

Podemos agrupar as vulnerabilidades nas seguintes categorias:

Falha do sistema

- Causa Complexidade;
- Atributos: Desenho pobre, falta de testes, operação

Falta de segurança

- Causa Financeira;
- Atributos Falta de atenção para protecção adequada

Factor humano

- Causa Ignorância
- Atributos Falta de consciência de segurança e/ou treinamento

Organizacional

- Causa Irresponsabilidade
- Atributos: Procedimentos e processos

Identificação de vulnerabilidades

O método comum para identificação de vulnerabilidades é com recurso a varredores (*scanners*):

Varredores de portas	*Nmap (Zenmap)*
Varredores de rede	*Nessus, OpenVAS*
Varredores web	*Nikto, OWASP ZAP, w3af*
Varredores de BD	*Scuba (Imperva), McAfee*
Varredores ERP	*ERPScan*

Classificação de vulnerabilidades

O nível de gravidade/severidade de uma vulnerabilidade é atribuído com base no risco de segurança imposto, caso a vulnerabilidade seja explorada, bem como o grau de dificuldade envolvido na sua exploração. O resultado de um ataque bem-sucedido ao explorar uma vulnerabilidade pode variar de negação de serviço e divulgação de informações a um comprometimento total de aplicativos ou sistemas.

- **Risco Crítico** *A exploração resulta em acesso root-level do sistema*
- **Risco alto** *A exploração resulta em acesso com privilégios elevados*
- **Risco médio** *A exploração resulta em acessos limitados*
- **Risco baixo** *A exploração afecta de forma muito limitada*
- **Informacional** *A exploração não afecta os sistemas*

Remediação de vulnerabilidades

Etapas básicas de remediação:

1. Confirmar que não tratasse de um falso positivo;
2. Testar o impacto da correcção (*patch*);
3. Desenvolver um plano de remediação;
4. Considerar controlos de mitigação;
5. Remediar de acordo com o plano;
6. Monitorar a execução do plano.

Priorização de vulnerabilidades

O plano de remediação deve fazer a priorização das vulnerabilidades de acordo com:

- **Grau de severidade da vulnerabilidade**

Ex: Vulnerabilidades de risco alto devem ser resolvidas o mais rápido possível.

- **Ambiente em que se encontra a vulnerabilidade**

Ex: Se o sistema vulnerável encontra-se de certo modo segregado, a sua correcção não é de grau alto

Mitigação de vulnerabilidades

Porque mitigar?

- Inexistência de *patch*;
- O *patch* pode causar impactos indesejados;
- O *patch* acarreta custos/recursos que não existem.

Como mitigar?

- Isolar o sistema (segregar);
- Alterar configuração especifica (*close unnecessary open ports*);
- Introduzir um sistema intermédio (*proxy, pass-through*).

Como manter uma rede saudável?

1. Implemente um sistema de monitoramento de ameaças;
2. Fazer testes (*scan*, *pentests*) regulares;
3. Estabelecer e forçar configurações padrão (*baseline*);
4. Fazer *hardening* dos sistemas;
5. Remediar vulnerabilidades.

Links de Interesse

1. https://www.cvedetails.com/
2. https://cve.mitre.org/
3. https://www.us-cert.gov/
4. https://thehackernews.com/
5. https://www.shodan.io/
6. *Vendor sites* (microsoft, cisco, adobe, oracle, ibm)

CERT-MZ

Tech Talk

Gestão de Vulnerabilidades

Q&A