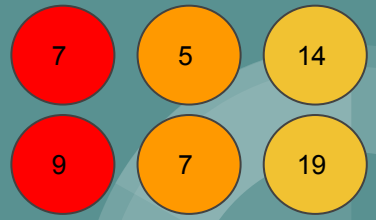
Análise de vulnerabilidades



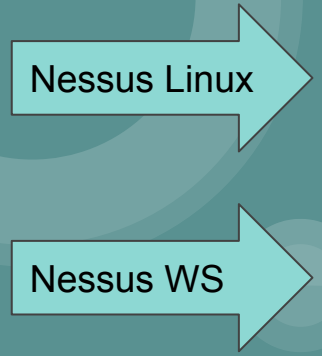
Resumo executivo

	Linux	Windows Server 2008 R2
Possibilidade de invasão por rede	Apresenta	Apresenta
Criação e execução de programas	Apresenta	Apresenta
Dados confidenciais vulneráveis	Não apresenta	Apresenta
Criação de contas no sistema	Apresenta	Apresenta

- Roubo de dados, golpes e fraudes
- Perda de credibilidade e danos à imagem
- Perda de espaço no mercado
- Prejuízos financeiros
- Processos judiciais e multas

Impacto potencial da vulnerabilidade

- **Acesso não autorizado ao sistema;**
- **Inserção de arquivos maliciosos no sistema;**
- **Criação de novas vulnerabilidades (Backdoor);**
- **Exposição de dados sigilosos;**
- **Alteração/exclusão de dados;**
- **Inserção de usuários falsos no sistema.**



Severity	CVSS v3.0	Plugin	Name
CRITICAL	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	7.5	34460	Unsupported Web Server Detection
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
CRITICAL	10.0	10203	rexecd Service Detection

Severity	CVSS v3.0	Plugin	Name
CRITICAL	7.5	34460	Unsupported Web Server Detection
CRITICAL	10.0	55883	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	138554	Microsoft DNS Server Remote Code Execution (SIGRed)
CRITICAL	10.0	108802	Microsoft Exchange Server Unsupported Version Detection (Uncredentialed)
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)

Opções de correção

- Criação/Melhoria do Firewall
- Senhas “mais fortes”
- Criptografia dos dados.
- Backup dos dados.
- Atualização de patch

Conclusão