

aals@cesar.school

Adyellen Alves
Lima da Silva



Estudo de caso

MICROSOFT EXCHANGE SERVER

1

DESCRIÇÃO, CONTEÚDO E IMPACTO

- Cadeia de vulnerabilidades críticas descobertas em **março de 2021** no **Microsoft Exchange Server**, permitindo **acesso remoto não autenticado e execução de código**.
- Motivação: espionagem cibernética e acesso a dados sensíveis de organizações (e-mails, credenciais, documentos).
- Utilizou técnicas avançadas de exploração de vulnerabilidades web (SSRF, deserialização insegura, escrita arbitrária de arquivos).

- Permitiu instalação de **web shells** e movimentação lateral, afetando empresas, governos e entidades no mundo todo.
- Um dos incidentes mais graves envolvendo software corporativo, com exploração em massa logo após a divulgação — **marco na história dos ataques contra infraestrutura de comunicação corporativa.**

2

TÁTICAS, TÉCNICAS E PROCEDIMENTOS(TTPS)

- **Reconhecimento:** busca por servidores Exchange expostos à internet (scans automatizados).
- **Initial Access:** exploração da vulnerabilidade CVE-2021-26855 (SSRF) para autenticação forjada.
- **Execução:** uso das falhas CVE-2021-26857 (deserialização insegura) e CVE-2021-27065/26858 para execução remota de código e gravação de web shells.
- **Persistência:** instalação de web shells (ex.: asp.net) nos diretórios do Exchange, garantindo acesso contínuo.
- **Escalada de privilégio:** abuso de permissões administrativas do Exchange para comprometer contas e serviços internos.

- **Movimentação lateral:** roubo de credenciais, exploração de AD e serviços internos após acesso inicial.
- **Collection & C2:** exfiltração de e-mails e dados sensíveis, comunicação remota via web shells para comandos adicionais.
- **Impacto:** comprometimento da confidencialidade (vazamento de dados), risco à integridade (alteração de configurações) e possibilidade de impacto na disponibilidade (uso posterior em campanhas de ransomware).

3

LABORATÓRIOS TRYHACKME

OhSINT:

<https://tryhackme.com/room/ohsint>

SSRF:

<https://tryhackme.com/room/ssrfhr>

Windows & Privilege Escalation:

https://tryhackme.com/room/window_s10privesc

Post-Exploitation & C2:

https://tryhackme.com/room/malmail_introductory

e

https://tryhackme.com/room/rppsem_pire