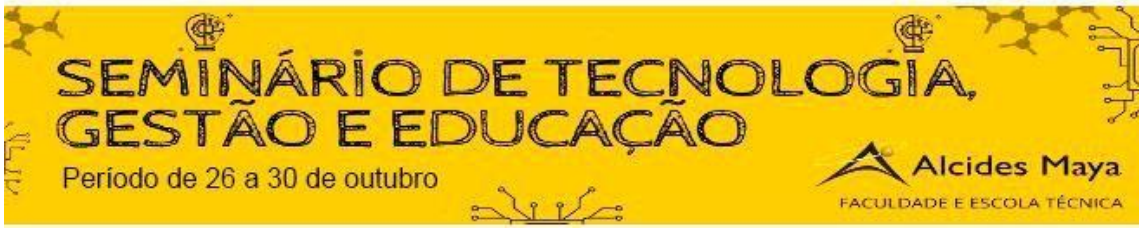

LOGON ZERO (CVE-2020-1472)

Rafael Araujo Bandeira[1]
Anderson santos da silva [2]
Inocêncio João Assis[3]

RESUMO

A empresa Microsoft apesar de ser uma referência mundial por sua praticidade e design, o fato de ter tantas funcionalidades apresentadas da maneira mais simples ao usuário sempre rendeu ao Windows bugs em atualizações e principalmente brechas aos cibercriminosos. Uma das mais recentes, que começou a ser estudada em agosto de 2020, é a chamada “logon zero”(CVE-2020-1472) vulnerabilidade do servidor Windows. A empresa, obviamente, mantendo seu padrão de qualidade, deixou patches de atualizações disponíveis em seu site oficial.

Palavras-Chave: cibercriminosos, logon, Microsoft, vulnerabilidade, Windows.

ABSTRACT

The Microsoft company despite being a world reference for its practicality and design, the fact that it has so many features presented in the simplest way to the user has always given Windows bugs in updates and mainly breaches to cybercriminals. One of the most recent, which began to be studied in August

[1]Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. rafael.10rafa@hotmail.com

[2]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. Anderson_silva@alcidesmaya.edu.br

[3]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. inocencio_assis@alcidesmaya.com.br

2020, is the so-called “zero logon” (CVE-2020-1472) Windows server vulnerability. The company, obviously, maintaining its quality standard, made update patches available on its official website.

Keywords: cybercriminals, login, Microsoft, vulnerability, Windows.

Como funciona esse ataque?

O logon zero está atrelado diretamente a um serviço do Windows Server: o Netlogon. Ele é o responsável por autenticar usuários, grupos e outros procedimentos advindos de controladores de domínio como o Active Directory. A falha consiste na possibilidade de um invasor se passar por um controlador de domínio e altera a senhas de usuários com acesso privilegiado, tendo acesso a alterar funções globais da ferramenta. Trata-se de uma vulnerabilidade de escalonamento de privilégios, não é uma falha que permite que o hacker invada a rede do Windows, porém é muito preciso como um ataque de dois estágios não dando possibilidade de defesa.

Em decorrência da criticidade do bug, a CISA (Agência de Segurança Cibernética e Infraestrutura) emitiu uma publicação de emergência ordenando que todas as agências civis federais dos EUA corrigissem a falha. Isso representa um “risco inaceitável” para os sistemas de TI do governo, dizia o alerta.

Como evitar ser hackeado?

A maneira mais efetiva de corrigir essa vulnerabilidade é instalando os patches de correção disponibilizados pela empresa. Manter seu Windows Server sempre atualizado através do **WSUS**, agendando as atualizações e avaliando o impacto de cada uma em sua estabilidade, é crucial para evitar ataques futuros envolvendo novas vulnerabilidades que, com certeza, surgirão. Embora burocrático e em alguns casos deixe o servidor indisponível por um tempo, não é um empecilho tão grande como perder totalmente seus dados e todo um

projeto organizacional, além de responder legalmente no caso de empresas que armazenam dados de clientes, fornecedores, entre outros.

Em junho desse ano, o Windows já havia lançado algumas atualizações e pretende finalizar esse novo projeto em combate ao logon zero até o início de 2021. Essas datas próximas, mostram como a segurança cibernética é essencial, já que hackers e invasores ficam à procura de brechas enquanto as encontradas são resolvidas.

REFERÊNCIAS

DM11 Segurança da Informação. Disponível em: https://dm11.com.br/vulnerabilidade-do-servidor-windows-logon-zero-identificada-pelo-invasor-patch-agora/ Acesso em: 21 de outubro 2020.

Microsoft. Disponível em: <https://docs.microsoft.com/pt-br/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus>. Acesso em: 21 de outubro 2020.