SEMINÁRIO DE TECNOLOGIA, GESTÃO E EDUCAÇÃO
Período de 26 a 30 de outubro
Alcides Maya
FACULDADE E ESCOLA TÉCNICA

VULNERABILIDADE SMB VERSÃO 1.0

Giancarlo Kologeski Kaminski1
Anderson santos da silva [2]
Roberto Bartzen Acosta [3]

RESUMO

Existe um protocolo, ativado por padrão no Windows, que tem mais de 30 anos e é extremamente suscetível a ataques. Uma de suas vulnerabilidades permitiu os ataques do WannaCry e Petya, que infectaram milhares de computadores em todo o mundo. Trata-se do SMB v1 (Server Message Block versão 1), antiga tecnologia usada para compartilhar arquivos em uma rede. E, recentemente, pesquisadores mostraram que uma falha nesse protocolo permite derrubar uma máquina com Windows através de um ataque de negação de serviço.
Palavras-chave: SMB, Windows, Compartilhamento, Ataque, Ransoware.

ABSTRACT

There is a protocol, activated by default in Windows, that is more than 30 years old and is extremely susceptible to attacks. One of its vulnerabilities allowed the attacks by WannaCry and Petya, which infected thousands of computers worldwide. This is SMB v1 (Server Message Block version 1), an old technology used to share files over a network. And recently, researchers have shown that a flaw in this protocol makes it possible to bring down a Windows machine through a denial of service attack.
Keywords: SMB, Windows, Sharing, Attack, Ransoware.

[1]Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. giancarlo.kaminski@alcidesmaya.edu.br
[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. roberto_acosta@alcidesmaya.edu.br

A vulnerabilidade do protocolo SMB permitiu o ataque do Ransomware (código malicioso que criptografa os dados da vítima e pede resgate pelo sequestro das informações) WannaCry, o qual ficou conhecido por infectar diversos computadores pessoais e de empresas. Chamada de “SMBloris”, não requer um computador potente para ser explorada, ela está presente em sistemas operacionais desde o Windows 2000, incluindo o Windows 10.

Não faltam motivos para tanto: o SMB v1 não é seguro (ele não tem suporte a criptografia); não é eficiente para comunicação em rede; e não é sequer necessário na maioria dos casos. Versões mais recentes, como SMB v2 e v3, são mais recomendáveis.

São raros os cenários em que ainda se usa a primeira versão do protocolo:

Se você ainda roda o Windows XP ou Server 2003 com suporte personalizado;

Se você tem um software antigo de gerenciamento que exige que os administradores usem navegadores desatualizados;

Se você usa impressoras multifuncionais antigas com firmware antigo para “escanear e compartilhar”.

Soluções

A maneira recomendada de corrigir um protocolo SMB vulnerável é instalar a atualização de segurança para o Microsoft Windows SMB server, publicada pela Microsoft no Boletim de Segurança MS17-010, em 14 de março de 2017.

Contudo, caso não seja possível prosseguir imediatamente com as atualizações necessárias, existem medidas alternativas que visam solucionar temporariamente as vulnerabilidades dos protocolos SMB. Desabilitar o Protocolo SMBv1, SMBv2 e SMBv3. É importante ressaltar que a Microsoft não recomenda a desativação dos protocolos SMBv2 e SMBv3. Caso a medida seja necessária, aconselha-se que seja apenas temporária. Bloquear o tráfego de entrada das portas TCP 137, 139 e 445 e das portas UDP 137 e 138.

REFERÊNCIAS

Jean Prado, WannaCry, que sequestra arquivos de PC<https://tecnoblog.net/214637/ransomware-wannacry-windows-smb-remover/> Acesso 23/10/2020;
Felipe Ventura, Ataque recurso antigo e inseguro do Windows <https://tecnoblog.net/221089/como-desativar-smb-v1-windows/> Acesso 24/10/2020;
SI UFRJ, HOST VULNERÁVEL USANDO O SERVIÇO SMB<https://www.security.ufrj.br/tutoriais/host-vulneravel-usando-o-servico-smb-aberto/> Acesso 24/10/2020.