-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Prezados,

O CAIS alerta para vulnerabilidades críticas recentes envolvendo o serviço Windows SMBv1 (Microsoft Server Message Block). Já existem códigos de exploração para a vulnerabilidade listada, como o "EternalBlue", o "EternalChampion", o "EternalRomance" e o "EternalSynergy".

Descrição

Um usuário malicioso não autenticado pode enviar pacotes especialmente criados a um servidor Windows SMBv1 alvo, permitindo a execução remota de código no processamento desses pacotes, podendo inclusive causar negação de serviço. Outra vulnerabilidade permite ao usuário malicioso não autenticado enviar pacotes maliciosos que podem resultar na divulgação não autorizada de informações do servidor Windows SMBv1.

Sistemas impactados

Microsoft Windows Vista
Microsoft Windows 7
Microsoft Windows 8.1
Microsoft Windows 10
Microsoft Windows Server 2008
Microsoft Windows Server 2012
Microsoft Windows Server 2016

Versões afetadas

Windows Vista Service Pack 2
Windows Vista x64 Edition Service Pack 2
Windows Server 2008 Service Pack 2 para sistemas de 32 bits
Windows Server 2008 Service Pack 2 para sistemas com base em x64
Windows Server 2008 Service Pack 2 para sistemas baseados em Itanium
Windows 7 Service Pack 1 para sistemas de 32 bits
Windows 7 Service Pack 1 para sistemas com base em x64
Windows Server 2008 R2 Service Pack 1 para sistemas com base em x64
Windows Server 2008 R2 Service Pack 1 para sistemas com base em Itanium
Windows 8.1 para sistemas de 32 bits
Windows 8.1 para sistemas com base em x64
Windows Server 2012 R2
Windows RT 8.1
Windows 10 para sistemas de 32 bits
Windows 10 para sistemas com base em x64

Windows Server 2016 para sistemas com base em x64
Windows Server 2008 Service Pack 2 para sistemas de 32 bits (instalação Server Core)
Windows Server 2008 Service Pack 2 para sistemas com base em x64 (instalação Server Core)
Windows Server 2008 R2 Service Pack 1 para sistemas com base em x64 (instalação Server Core)
Windows Server 2012 (instalação Server Core)
Windows Server 2012 R2 (instalação Server Core)
Windows Server 2016 para sistemas com base em x64 (instalação Server Core)

Correções disponíveis

Para mitigar o problema, recomenda-se desabilitar o recurso SMBv1 nos sistemas Windows. Também é possível aplicar regras de controle de acesso do tráfego de rede para as portas TCP 139 e 445 e UDP 137 e 138. Vale ressaltar que tais regras devem ser avaliadas de acordo com o ambiente em questão. Para correção da vulnerabilidade, é necessário aplicar as atualizações de segurança disponibilizadas pela Microsoft através do sistema Windows Update.

Identificadores CVE (http://cvw.mitre.org)

CVE-2017-0143
CVE-2017-0144
CVE-2017-0145
CVE-2017-0146
CVE-2017-0147
CVE-2017-0148

Mais informações

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0146
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148
https://technet.microsoft.com/pt-br/library/security/ms17-010.aspx
https://support.microsoft.com/pt-br/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012
https://isc.sans.edu/forums/diary/ETERNALBLUE+Windows+SMBv1+Exploit+Patched/22304/
https://www.us-cert.gov/ncas/current-activity/2017/03/16/Microsoft-SMBv1-Vulnerability

https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.

Os alertas do CAIS também podem ser acompanahadas pelas redes sociais da RNP. Siga-nos!!
Twitter: @RedeRNP
Facebook: facebook.com/RedeNacionaldeEnsinoePesquisaRNP.

Atenciosamente,

CAIS/RNP


```
#################################################################
#   CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)      #
#       Rede Nacional de Ensino e Pesquisa (RNP)                #
#                                                               #
# cais@cais.rnp.br       http://www.rnp.br/servicos/seguranca   #
# Tel. 019-37873300      Fax. 019-37873301                       #
# Chave PGP disponivel   http://www.rnp.br/cais/cais-pgp.key    #
#################################################################
```



```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQCUAwUBWPewu+kli63F4U8VAQIaRAP2MC9oVAy/yMcPzRlE3VcWmphkltEeGp6b
4azo0k15hcFMP4t1GypJgMH1OYnbtnzXIiPSEIUFcMVIYSCKEI1H8xtH7eE3+8Qb
741QwHBnmpiPi7avzhqcL1X3VywK97lYKq38z4Hr8KAQmmoRlgya0pEc0nh5BZX8
nS3Wo+N2pA==
=nZ1l
-----END PGP SIGNATURE-----
```