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

Prezados,

O CAIS alerta para vulnerabilidades críticas recentes envolvendo o kernel do sistema operacional Windows que podem permitir
elevação de privilégios e execução de códigos maliciosos. Até o momento da divulgação deste alerta, não foram divulgados
códigos de exploração para as vulnerabilidades listadas.

Descrição

Um usuário malicioso, através da execução de um arquivo especificamente desenvolvido, pode assumir o controle total do
sistema afetado através da elevação de privilégios.

Vulnerabilidades existentes no gerenciamento de objetos alocados em memória quando o driver de modo kernel do Windows
manipula incorretamente objetos na memória permite ao atacante executar código arbitrário, possibilitando ao usuário
malicioso instalar programas, exibir, alterar, excluir dados e criar novas contas com privilégios administrativos.

Outra vulnerabilidade existente no kernel do Windows permite ao usuário malicioso executar processos com privilégios elevados
quando o Gerenciador de Transação do Windows (KTM) manipula indevidamente objetos criados na memória, permitindo ao atacante
obter privilégios quando o Windows não consegue verificar o comprimento de um buffer antes da cópia de blocos de memória.

Para explorar essas vulnerabilidades, o atacante precisa ter uma sessão de autenticação (logon) iniciada e executar um
aplicativo especialmente criado para realizar a elevação de privilégio e assumir o controle total do sistema. Um usuário do
sistema pode ser induzido a executar esses aplicativos através de arquivos maliciosos compartilhados ou códigos enviados por
e-mails ou sites web suspeitos.

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
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

É necessário aplicar as atualizações de segurança disponibilizadas pela Microsoft através do sistema Windows Update. É
recomendada a reinicialização do sistema para aplicação das atualizações.

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

CVE-2017-0024
CVE-2017-0026
CVE-2017-0050
CVE-2017-0056
CVE-2017-0078
CVE-2017-0079
CVE-2017-0080
CVE-2017-0081
CVE-2017-0082
CVE-2017-0101
CVE-2017-0102
CVE-2017-0103

Mais informações

https://technet.microsoft.com/pt-br/library/security/ms17-017
https://technet.microsoft.com/pt-br/library/security/ms17-018

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

iQCVAwUBWPkQuukli63F4U8VAQIwGQQAgvITqkgBt1X2grrJH//WAtSS0pRJ80Sf
Ep2qTNJc33rGiSZEFl7SCIMA2rohvIDBcJZqgpfdOJGjuCtAOW3djjDRKpkyhpMC
y6dPKrFpTrjHxvaJ3lckhApIur+SRhC5P4mY+U7ghWZJFdL5FQuilL1MQHFg8a0B
W3bsOgRYkgM=
=fGc9
-----END PGP SIGNATURE-----