-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Prezados,

O CAIS alerta para a recente vulnerabilidade encontrada no mecanismo de proteção contra malwares da Microsoft (MMPE - Microsoft Malware Protection Engine), que é fornecido com vários produtos de proteção contra vírus da Microsoft, como, por exemplo, o Windows Defender, Microsoft Endpoit Protection, Security Essentials, entre outros. Esta vulnerabilidade permite a execução remota de códigos maliciosos e o controle total do computador por um usuário malicioso. Já foram publicados códigos de exploração para a vulnerabilidade listada.

Descrição

Um usuário malicioso, através de um arquivo especificamente desenvolvido, pode assumir o controle total do sistema afetado através da execução de códigos no contexto de segurança da conta LocalSystem e assim assumir o controle total do sistema. A exploração dessa vulnerabilidade ocorre no momento que este arquivo é verificado pelo mecanismo de proteção contra malwares da Microsoft (MMPE), não sendo, no entanto, condição necessária abrir ou executar o arquivo malicioso.

Uma vez que os produtos que executam o MMPE, por padrão, tem a funcionalidade de verificação em tempo real ativada (o que significa que os arquivos assim que são criados, abertos, copiados ou descarregados em um sistema são escaneados imediatamente pelo sistema), um atacante pode executar o código de exploração no sistema afetado de diversas maneiras. Por exemplo, o atacante pode utilizar um site que contenha o arquivo e enviar o link para a vítima, que ao acessá-lo, inicia o escanamento pela ferramenta de proteção da Microsoft. O atacante pode também enviar de uma mensagem de e-mail que possui em anexo o arquivo malicioso, e a vítima, assim que receber a mensagem, sem necessariamente precisar abrí-la, inicia a verificação pelo MMPE. Outra forma é a vítima receber o arquivo malicioso através de uma mensagem enviada por algum aplicativo de mensagens instantâneas (por exemplo, Skype, Pidgin, Whatsapp Messenger, entre outros), cuja verificação é iniciada no momento que o arquivo é recebido. Além disso, a vulnerabilidade pode ser explorada também em servidores de hospedagem de arquivos, onde o atacante pode realizar o upload do arquivo malicioso para um local compartilhado, fazendo que o sistema execute a verificação do MMPE no servidor.

O usuário malicioso não precisa estar na mesma rede local que o sistema vulnerável, o que significa que os sistemas Windows podem ser explorados remotamente a partir de qualquer lugar. Outra característica do ataque é a possibilidade dele se espalhar, uma vez que ao tomar o controle administrativo do computador, o atacante pode automaticamente usá-lo para enviar o arquivo malicioso para outros sistemas através de compartilhamentos locais abertos.

Mesmo se a verificação automática em tempo real do MMPE não estiver ativada, a exploração da vulnerabilidade pode ocorrer em uma próxima verificação agendada. Todos os sistemas que executam uma versão afetada do MMPE estão em risco.

Sistemas impactados

Windows 7
Windows 8

Windows 8.1
Windows RT 8.1
Windows 10
Windows 2016

Produtos afetados

Microsoft Forefront Endpoint Protection 2010.
Microsoft Endpoit Protection.
Microsoft Forefront Security for SharePoint Service Pack 3.
Microsoft System Center Endpoint Protection.
Microsoft Security Essentials.
WIndows Defender for Windows 7.
Windows Defender for Windows 8.1.
Windows Defender for Windows RT 8.1.
Windows Defender for Windows 10.
Windows Defender for Windows Server 2016.
Windows Intune Endpoint Protection.

Correções disponíveis

É necessário executar a atualização dos produtos afetados que utilizam a proteção contra malwares da Microsoft, bem como também 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-2017-0290

Mais informações

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0290
https://technet.microsoft.com/library/security/4022344
http://thehackernews.com/2017/05/windows-rce-exploit.html
http://thehackernews.com/2017/05/windows-defender-rce-flaw.html
http://thehackernews.com/2017/05/patch-windows-zero-days.html
https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5 (exploit)

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

iQCVAwUBWRRldukli63F4U8VAQJ22gP+MZDr95hZDRp8T1ZaxS56LjSNfLncUd5e
XzdoymowYyW1Mvi1/vMOV3Ej0k9YfiDJW6gezrCTNnQdjO5XbOkgiw2n6/Ss1/cr
nixIRVTZPOFHorDXnImZ2TSjWHQ1TZDEtBWYxVzG/a46o2G1GMfK0jIXV6YOvvCn
unsh31z0r4E=
=7U1K
-----END PGP SIGNATURE-----