CAIS-ALERTA [12/12/2017]: Vulnerabilidade crítica no sistema Microsoft Malware Protection

Prezados,

O CAIS alerta para vulnerabilidade recente envolvendo o sistema de proteção contra malware da Microsoft, o Microsoft Malware Protection, o qual provê as capacidades de varredura, detecção e limpeza para a suíte de softwares antimalwares da Microsoft. Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para a vulnerabilidade listada.

DESCRIÇÃO

Uma vulnerabilidade na engine do Microsoft Malware Protection permite controle administrativo total do sistema operacional Windows através da execução de código remoto. Um usuário malicioso pode introduzir um arquivo malicioso especialmente desenvolvido no sistema, o qual causa corrupção de memória quando executada a varredura nele.

A exploração da vulnerabilidade ocorre quando a engine do Microsoft Malware Protect não examina corretamente um arquivo especialmente criado. Um usuário malicioso que consiga explorar essa vulnerabilidade pode ganhar controle total sobre o sistema operacional Windows e executar uma série de tarefas maliciosas, como instalação de softwares, acessar, modificar e/ou apagar dados e criar outras contas com privilégios administrativos no sistema utilizando a conta LocalSystem.

SISTEMAS AFETADOS

Todas as versões do sistema operacional Windows que executam os seguintes softwares:
- - Microsoft Exchange Server 2013 and 2016
- - Microsoft Forefront Endpoint Protection
- - Microsoft Security Essentials
- - Windows Defender for Windows 7, Windows 8.1, Windows 10 and Windows Server 2016
- - Windows Intune Endpoint Protection

CORREÇÕES DISPONÍVEIS

Atualizar o mais breve possível a engine e assinaturas do Microsoft Protection Engine para a versão 1.1.14405.2 ou a mais recente disponibilizada pela Microsoft em todos os sistemas afetados pela vulnerabilidade.
É recomendada a reinicialização do sistema após a aplicação das atualizações.

IDENTIFICADORES CVE

CVE-2017-11937

MAIS INFORMAÇÕES

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11937
https://thehackernews.com/2017/12/windows-update-malware-protection.html

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 são oferecidos no Twitter:
Siga @caisrnp

Atenciosamente,

CAIS/RNP


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