CAIS-ALERTA [15/03/2018]: Vulnerabilidade no protocolo CredSSP

O CAIS alerta para a recente vulnerabilidade encontrada no protocolo CredSSP, utilizado pelo serviço de área de trabalho remota do Microsoft Windows. Até o momento da publicação deste alerta, não foram identificados códigos de exploração para a vulnerabilidade identificada.

DESCRIÇÃO

O protocolo CredSSP (Credential Security Support Provider - Provedor de suporte a credencial segura) é utilizado pelo RDP (Remote Desktop Protocol - Protocolo de área de trabalho remota) e pelo WinRM (Windows Remote Management - Gerenciamento remoto do Windows) para encaminhar credenciais de acesso de forma segura (cifrada) de um cliente Windows para servidores que farão sua autenticação remota.

A falha ocorre na função de cifragem do CredSSP, que pode ser explorada através de um ataque de interceptação (Man-in-the-middle - MITM), em uma rede cabeada ou wifi, para retransmitir as credenciais de um usuário que teve sua sessão sequestrada (session hijacking) e executar comandos no servidor de destino.

SISTEMAS IMPACTADOS

Serviços RDP e WinRM

VERSÕES AFETADAS

Todas as versões do Microsoft Windows

CORREÇÕES DISPONÍVEIS

Atualizar o Sistema Operacional Windows (clientes e servidores) com as últimas correções disponibilizadas pela Microsoft, e seguir os procedimentos do boletim em [2], Seção Diretiva de Grupo;
Atenção ao fato que, caso cliente e servidores não estejam devidamente atualizados, falhas de comunicação podem ocorrer.

IDENTIFICADORES CVE (http://cve.mitre.org)

CVE-2018-0886

MAIS INFORMAÇÕES

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0886
[2] https://support.microsoft.com/pt-br/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018
[3] https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-0886

[4] https://blog.preempt.com/security-advisory-credssp

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 acompanhados pelas redes sociais da RNP. Siga-nos!
Twitter: @RedeRNP
Facebook: facebook.com/RedeNacionaldeEnsinoePesquisaRNP.


```
#################################################################
#   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   https://www.cais.rnp.br/cais-pgp.key   #
#################################################################
```