CAIS-ALERTA [13/03/2018]: Vulnerabilidades no serviço LDAP Samba

O CAIS alerta para a recente vulnerabilidade encontrada no serviço Samba que pode permitir a alteração de senha de qualquer conta em sua base de dados. Até o momento da publicação deste alerta, não foram identificados códigos de exploração para as vulnerabilidades identificadas.

DESCRIÇÃO

Um servidor Samba vulnerável configurado no domínio como AD DC (Active Directory Domain Controller) não valida corretamente as permissões ao modificar senhas via LDAP, permitindo que usuários autenticados alterem remotamente senhas de outros usuários, incluindo usuários administrativos ou contas com privilégios de serviços.

Por padrão, usuários autenticados tem permissão de alteração de senha somente para seu próprio objeto 'usuário' (self). O servidor Samba vulnerável não valida corretamente a solicitação de alteração de senha concedendo permissão global (world/everyone), permitindo assim executar, ao invés da operação de modificação de senha do próprio objeto 'usuário', uma operação de redefinição de senha para qualquer outro objeto LDAP. A janela do Windows mostra isso como o direito "Alterar senha" concedido a "Todos".

SISTEMAS IMPACTADOS

Serviço Samba LDAP

VERSÕES AFETADAS

Todas as versões a partir da 4.0.0

CORREÇÕES DISPONÍVEIS

Atualizar o Servidor Samba para as versões 4.7.6, 4.6.14, ou 4.5.16.
Dentre as soluções de contorno para evitar a exploração da vulnerabilidade, estão:
1) A aplicação de scripts que revogam os direitos de alteração de senhas, permitindo que o usuário tenha possibilidade de alterar somente a senha de sua própria conta;
2) Desabilitar o serviço LDAP.
Os comandos e as implicações da aplicação das soluções de contorno mencionadas podem ser encontradas na Wiki do Samba, na seção 'MAIS INFORMAÇÕES'.

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

CVE-2018-1057

MAIS INFORMAÇÕES

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1057
https://www.samba.org/samba/security/CVE-2018-1057.html
https://wiki.samba.org/index.php/CVE-2018-1057:_Unprivileged_user_can_change_any_user_.28and_admin.29_password
https://thehackernews.com/2018/03/samba-server-vulnerability.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 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   #
#################################################################
```