CAIS-ALERTA [26/03/2018]: Vulnerabilidades na Suíte de Colaboração Zimbra

O CAIS alerta para a recente vulnerabilidade encontrada no serviço ZIMBRA (ZCS), que pode permitir uma ampla variedade de ações maliciosas que visam executar tarefas em nome de usuários e coletar credenciais de acesso. Já foram desenvolvidos códigos de exploração para a vulnerabilidade identificada.

DESCRIÇÃO

Uma vulnerabilidade Cross-Site Scripting (XSS) pode permitir a um usuário malicioso executar ações em nome de outros usuários ou apresentar uma tela de login falsa para coletar informações como nome de usuários e senhas. Para cada e-mail que contém anexos aberto no Zimbra, este executa uma função que cria um link para cada um deles. Porém nenhuma verificação é executada e o valor do cabeçalho pode ser modificado ou influenciado por um usuário malicioso, o qual pode injetar um código HTML ou JavaScript na tag do link. Para explorar essa vulnerabilidade, o usuário malicioso envia a um usuário do Zimbra um e-mail com um cabeçalho modificado. Quando a mensagem é aberta, o script malicioso é executado.

SISTEMAS IMPACTADOS

Zimbra Collaboration Suite (ZCS).

VERSÕES AFETADAS

Versão 8.5.0 e versões posteriores.

CORREÇÕES DISPONÍVEIS

Atualizar a versão da suíte do Zimbra (ZCS) para a versão 8.8.7.

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

CVE-2018-6882

MAIS INFORMAÇÕES

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2018-6882
https://www.securify.nl/advisory/SFY20180101/cross-site-scripting-vulnerability-in-zimbra-collaboration-suite-due-to-the-way-it-handles-attachment-links.html
https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.7
https://bugzilla.zimbra.com/show_bug.cgi?id=108786
https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

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       #
#####################################################################
```