CAIS-ALERTA [22/03/2018]: Vulnerabilidades no Citrix XenServer

O CAIS alerta para as recentes vulnerabilidades anunciadas no Citrix XenServer. Até o momento da publicação deste alerta, não foram identificados códigos de exploração para a vulnerabilidade identificada.

DESCRIÇÃO

Foram identificadas vulnerabilidades que podem, se exploradas, indisponibilizar ou comprometer o sistema Host:

Uma falha de estouro de buffer (buffer overflow) no Openvswitch permite execução de código arbitrário através de pacotes MPLS manipulados; outras falhas, ainda, podem causar negação de serviço (DoS) através de alto consumo de CPU ou travamento no hypervisor.

SISTEMAS IMPACTADOS

Sistema de virtualização XenServer

VERSÕES AFETADAS

Todas as versões do Citrix XenServer anteriores a 7.4

CORREÇÕES DISPONÍVEIS

Aplicar as correções (hotfixes) disponibilizadas pela Citrix, conforme boletim em [4].

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

CVE-2016-2074: openvswitch: MPLS buffer overflow vulnerability
CVE-2018-7540: DoS via non-preemptable L3/L4 pagetable freeing
CVE-2018-7541: grant table v2 -> v1 transition may crash Xen

MAIS INFORMAÇÕES

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2074
[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7540
[3] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7541
[4] https://support.citrix.com/article/CTX232655

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
###