

Prezados,

O CAIS alerta para a vulnerabilidade crítica recente envolvendo o framework para aplicações web Apache Struts 2.

Exploits de prova de conceito (PoC) já foram divulgados publicamente, o que torna ainda mais urgente a atualização.

#### Descrição

O Apache Struts é um framework MVC (model-view-controller) de desenvolvimento da camada controladora de aplicações web, construído em Java para ser usado como container web em um servidor J2EE. Uma vulnerabilidade no framework permite a execução remota de códigos, permitindo que atacantes, sem autenticação e relativa facilidade, executar comandos diretamente no sistema operacional do servidor Web. Sistemas que utilizam o Struts, como Tomcat e JBoss, entre outros, podem ser comprometidos.

#### Sistemas impactados

Sistemas utilizando o Apache Struts nas versões 2 (2.3.5 – 2.3.31) e 2.5 (2.5 – 2.5.10)

#### Versões afetadas

Versões anteriores a 2.3.32 e 2.5.10.1

#### Correções disponíveis

Atualizar a versão do framework Java Apache Struts para a versão mais recente disponibilizada pelos desenvolvedores (2.3.32 e 2.5.10.1, no momento da publicação deste alerta) ou a versão mais recente recomendada de acordo com o sistema operacional em uso. É recomendada a reinicialização do servidor Web (aplicação da correção acontece após a atualização).

Identificadores CVE (<http://cvw.mitre.org>)

CVE-2017-5638

#### Mais informações

<http://www.securityfocus.com/bid/96729>

<https://security-tracker.debian.org/tracker/CVE-2017-5638>

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