CAIS-Alerta [17/01/2018]: Vulnerabilidade no BIND 9

Prezados,

O CAIS alerta para vulnerabilidade recente envolvendo o servidor de nomes (DNS) BIND9. Até o momento da divulgação deste alerta, não foram divulgados códigos de exploração para a vulnerabilidade listada.

Descrição

O servidor de nomes (DNS) BIND não efetua corretamente a limpeza de dados na memória para consultas recursivas quando valida DNSSEC. Um usuário malicioso ao identificar que o servidor BIND está com esse recurso ativo poderia criar uma requisição DNS maliciosa e causar falha no serviço e consequentemente sua indisponibilidade.

Sistemas impactados

BIND 9

Versões afetadas

Todas versões do BIND a partir de 9.0.0

Correções disponíveis

Atualizar a versão do BIND para a mais recente disponibilizada pelos desenvolvedores ou a versão mais recente de acordo com o sistema em uso.
Uma solução de contorno consiste na desativação da validação de DNSSEC até que os patches de correção sejam devidamente aplicados ou o ambiente seja atualizado.

É recomendada a reinicialização do serviço.

Identificadores CVE (http://cve.mitre.org)
CVE-2017-3145

Mais informações
https://kb.isc.org/article/AA-01542

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