-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

CAIS-Alerta [03/07/2017]: 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

Um usuário malicioso que tiver conhecimento de uma chave TSIG (Transaction Signature - protocolo usado pelo serviço DNS para prover um meio de autenticação à base de dados dos registros) e tiver permissão para enviar e receber mensagens para um DNS autoritativo, pode ser capaz de manipular o BIND para aceitar e processar uma atualização dinâmica não-autorizada. Servidores que dependem exclusivamente de chaves TSIG para proteção, sem ACLs para validar acessos baseados em endereços de rede, podem ser vulneráveis à manipulação maliciosa de conteúdo de zonas utilizando a técnica descrita anteriormente.

Sistemas impactados

BIND 9

Versões afetadas

9.4.0 até 9.8.8
9.9.0 até 9.9.10-P1
9.10.0 até 9.10.5-P1
9.11.0 até 9.11.1-P1
9.9.3-S1 até 9.9.10-S2
9.10.5-S1 até 9.10.5-S2

Correções disponíveis

Atualizar a versão do BIND para a mais recente disponibilizada pelos desenvolvedores ou a versão mais recente de acordo com o sistema operacional em uso. Uma solução de contorno consiste no uso de ACLs (Access Control Lists) para exigir a validação de endereços de rede juntamente com autenticação TSIG.

É recomendada a reinicialização do serviço.

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

CVE-2017-3143

Mais informações

https://kb.isc.org/article/AA-01503
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3143
https://kb.isc.org/article/AA-00723/0/Using-Access-Control-Lists-ACLs-with-both-addresses-and-keys.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 acompanahadas 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    #
#################################################################
```


-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1

iQCVAwUBWVqZyOkli63F4U8VAQK5IwQArLa6QPompjZQCJbfZIg15fPazshQ+Bz6

KDe1ZoZ/p9vcnWvDqpKqXnkBB6VQn9ecc3gIJKjqJ6yAl0Ind9Q+SP9eaFbstiod

drFy7pSpiMjtEsha1lwfD0ztltyOzaOLIkUCX05RPfUPAJzXGzWGfg4jtjN30wyL

2ARdlZ0HKP4=

=KCh9

-----END PGP SIGNATURE-----