CAIS-Alerta: Vulnerabilidades no BIND

[RNP, 12.12.2014]

O CAIS está repassando dois alertas do ISC (Internet Systems Consortium), intitulados "CVE-2014-8500: A Defect in Delegation Handling Can Be Exploited to Crash BIND" e "CVE-2014-8680: Defects in GeoIP features can cause BIND to crash", que tratam de diversas vulnerabilidades no servidor DNS BIND.

Até o momento da publicação desse alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

DESCRIÇÃO:

CVE-2014-8500 - A Defect in Delegation Handling Can Be Exploited to Crash BIND: Um usuário mal intencionado pode causar a indisponibilidade/exaustão de recursos (DoS) ao realizar consultas especificamente construídas fazendo com o que o servidor BIND efetue ilimitadas requisições ao tentar resolver tais consultas de forma recursiva.

SISTEMAS IMPACTADOS

Todos os servidores com recurso de consultas recursivas habilitadas são afetados. Servidores autoritativos também podem ser afetados, porém o atacante necessita obter controle sob uma zona delegada abaixo desse servidor.

VERSÕES AFETADAS:

9.0.x até 9.8.x;

9.9.0 até 9.9.6;

9.10.0 até 9.10.1

CORREÇÕES DISPONÍVEIS

Atualizar a versão do BIND para a versão mais recentes, aplicar as correções disponíveis no site do ISC ou do suporte do seu sistema operacional.

DESCRIÇÃO:

CVE-2014-8680 - Defects in GeoIP features can cause BIND to crash:

Diversas vulnerabilidades relacionadas a função de GeoIP na versão 9.10.x do ISC BIND. Algumas dessas vulnerabilidades podem até causar indisponibilidade/exaustão de recursos (DoS).

SISTEMAS IMPACTADOS:

Todos os servidores que fazem uso do recurso de GeoIP são impactados.

VERSÕES AFETADAS

9.10.0 até 9.10.1

CORREÇÕES DISPONÍVEIS

Atualizar a versão do BIND para a versão mais recentes, aplicar as correções disponíveis no site do ISC ou do suporte do seu sistema operacional.

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

CVE-2014-8680, CVE-2014-8680

MAIS INFORMAÇÕES

https://kb.isc.org/article/AA-01216/

https://kb.isc.org/article/AA-01217/

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 são oferecidos no formato RSS/RDF e no Twitter:

http://www.rnp.br/cais/alertas/rss.xml

Siga @cais_rnp.

##

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 #

##