Alerta de Segurança 002/2012 - CGTI/VPGDI

Em 26 de março de 2012

Para: Gestor de TI

Assunto: DNS reverso aberto

Prezado Gestor,

Nos últimos dias recebemos um grande volume de notificações do Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP) a respeito de hosts da Fiocruz configurados como DNS recursivo aberto.

O DNS (*Domain Name Service*) se tornou um serviço crítico e indispensável para garantir a disponibilidade e o uso adequado da Internet, efetuando a resolução de nomes de domínios em endereços IP e vice-versa.

Entretanto, o DNS apresenta uma série de vulnerabilidades que, se não forem tratadas, podem comprometer todo o sistema de nomes de domínio. Uma vulnerabilidade muito comum de configuração é o servidor de DNS recursivo aberto, que permite a qualquer host na Internet fazer consultas ao servidor DNS de uma rede externa. Neste contexto, os servidores de DNS recursivos abertos estão suscetíveis a sofrer os seguintes ataques:

- Envenenamento de cache (*cache poisoning*): levam o servidor recursivo a armazenar informações forjadas. Uma vez envenenado, o atacante usa o servidor web para efetuar, entre outros, ataques de *phishing* ou disseminar *malware*;
- Negação de Serviços Distribuídos (*DDoS – Distributed Denial Of Service*): consiste no envio de um número elevado de perguntas recursivas a um ou mais servidores de DNS, provocando um esgotamento de recursos como a largura de banda disponível, espaço de memória ou capacidade de processamento do servidor;
- Ser utilizado por sistemas externos a sua rede, consumindo recursos computacionais internos.

Sendo assim, visando mitigar os riscos associados ao serviço de DNS, o Serviço de Segurança da Informação e Comunicações da CGTI recomenda separar os servidores autoritativo e recursivo e atribuir políticas de acesso distintas. Para isso duas soluções podem ser adotada:

- Separar os servidores de DNS em computadores diferentes (com configurações e políticas de acesso distintas). Neste caso os registros NS das zonas servidas devem apontar apenas para os servidores autoritativos;
- Adotar o conceito de visões (*views*), definindo ao menos duas *views* possíveis para o servidor DNS, uma para acesso de clientes específicos e outra para acesso por parte da Internet como um todo. É importante definir a ordem das *views*, sempre da mais específica para a mais geral;

Mais informações sobre a implementação das ações podem ser encontradas no endereço http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Atenciosamente,

Misael Sousa de Araujo
Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações

Misael Sousa de Araujo
CGTI/VPGDI
Matrícula SIAPE 1559383