CAIS-Alerta: ataques de negação de serviço envolvendo o abuso de servidores NTP - Atualização 1

[RNP, 30.05.2014-, revisão 01]

O CAIS publicou, no dia 22 de janeiro de 2014, um alerta sobre a vulnerabilidade envolvendo consultas do tipo "monlist" em servidores NTP, porém há registro de exploração de uma nova vulnerabilidade envolvendo servidores NTP. Diante disso, o CAIS lança uma atualização do alerta "Ataques de negação de serviço envolvendo o abuso de servidores NTP".

O novo problema está relacionado a uma configuração incorreta do servidor NTP que permite a execução remota do comando "READVAR" (comando que exibe dados como: versão do NTP, versão do sistema operacional entre outros)

Embora, o problema não seja tão grave quanto a consulta Modo 7 para MONLIST, as consultas para READVAR podem fornecer amplificação em torno de 30 vezes.

Impacto

Um usuário malicioso poderia forjar um endereço IP de origem e executar remotamente esse comando em algum servidor NTP vulnerável. O servidor NTP vulnerável, por sua vez, iria responder essa consulta com um pacote, aproximadamente, 30 vezes maior que o pacote inicial. Assim, o servidor que teve seu IP forjado seria inundado de informações não solicitadas, sofrendo um ataque reflexivo distribuído de negação de serviço.

Recomendações

- O CAIS recomenda que, ao menos, uma das soluções abaixo sejam executadas para proteger seu servidor NTP contra ataques de negação de serviço, envolvendo consultas do tipo "READVAR" e do tipo "monlist":
- Atualizar o servidor NTP para a versão "NTP version 4.2.7"
-
- Seguir o template de configuração segura disponibilizado pelo Team-Cymru do serviço NTP. O template apresenta soluções para os seguintes sistemas: Cisco IOS, Juniper Junos e UNIX ntpd.
-
- Seguir as recomendações de Hardening para Roteadores Cisco.
-
- Seguir as recomendações da empresa RAPID 7.

Ferramentas para consultas

- A equipe do CAIS identificou algumas ferramentas, para que os administradores de sistemas consultem o status de seus servidores NTP. Através dessas, é possível identificar um servidor NTP vulnerável.

  # Específico para vulnerabilidade "monlist"

- Site oficial do OpenNTPProject que identifica servidores NTP vulneráveis (a atualização dos dados é feita semanalmente).
- Executar um dos comandos abaixo para identificar se seu servidor NTP está vulnerável. Caso o comando retorne uma lista de endereços IPs após a execução, seu servidor está vulnerável.
- # ntpdc -n -c monlist "endereço IP do servidor NTP"

  # ntpq -c rv "endereço IP do servidor NTP"

- Executar a ferramenta Nmap, conforme instruções abaixo:

  nmap -sU -p U:123 -n -Pn --script ntp-monlist "Endereço IP"

- **# Específico para vulnerabilidade "READVAR"**

  Para verificar se seu servidor está vulnerável, execute as rotinas abaixo:

- Instalar o NTPQ em uma máquina fora da sua rede
- Executar o aplicativo
- # ntpq
- Informar o host que deseja verificar
- # host "endereço IP"
- 4 - Executar a consulta READVAR
- # readvar

  Se a consulta não retornar "timeout", seu servidor está vulnerável. Deste modo, siga as recomendações acima para configurá-lo de forma segura.

Mais informações

- CAIS-Alerta: ataques de negação de serviço envolvendo o abuso de servidores NTP
- Ameaças de NTP impulsionam DDoS
- Understanding and mitigating NTP-based DDoS attacks
- NTP Amplification DDoS Attacks

- Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks
- Página do ShadowServer sobre vulnerabilidade "READVAR"

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 @caisrnp.