Misbruik

NTP Reflection DDoS attacks

Uw internetverbinding is recent misbruikt voor NTP reflection en DDoS aanvallen.

Door gebruik te maken van een bug en standaard open instellingen van de NTP deamon is het mogelijk om een DDoS aanval uit te voeren als er geen source IP adres verificatie is. Hierbij spooft de aanvaller het source IP adres van de pakketjes richting de NTP daemon die reageert door een antwoord te sturen naar een machine die de aanval ontvangt. De ontvangende machine word bestookt met een grote hoeveelheid data omdat de reactie van de server vele malen groter is dan de oorspronkelijke aanvraag.

Is mijn server ook onderdeel van dit probleem?

Mogelijk wel, echter zijn er een aantal dingen die u kunt doen om dit probleem op te lossen.

Stap 1: Is uw besturingssyteem up-to-date?
Allereerst moet u ervoor zorgen dat het besturingssysteem up-to-date is en dat alle updates geïnstalleerd zijn, de bug in de NTP deamon stamt uit 2010 en nieuwere versies zijn niet gevoelig voor deze aanval.

Stap 2: Is uw systeem versie correct?
Controleer of uw eigen server gevoelig is.
Vanaf uw (Linux/FreeBSD server):
ntpd --version

Hiermee ziet u de versie van NTP, deze moet dus 4.2.7p26 of hoger zijn, alternatief:

ntpdc -n -c monlist localhost

Als u een lijst met server adressen ziet reageert uw server op de MONLIST aanval!

Stap 3: Verhelpen kwetsbaarheid
Om de kwetsbaarheden te verhelpen dient u het besturingsysteem bij te werken.

Als uw server nog gevoelig blijkt dan kunt u de volgende regels aanpassen of toevoegen in /etc/ntp.conf (in Debian)

restrict -4 default nomodify nopeer noquery notrap
restrict -6 default nomodify nopeer noquery notrap
disable monitor

Indien u NTP niet naar het internet serveert gebruik dan ook de volgende regel:

restrict 127.0.0.1
restrict ::1

Vergeet niet de NTP deamon te herstarten om de wijzigingen door te voeren.

/etc/init.d/ntp restart

Verifieer met:ntpdc -n -c monlist localhostof de wijziging succesvol is.

Een alternatief is de firewall regels zo in te stellen dat er geen verkeer van UDP poort 123 naar buiten toe sessies mag opzetten.

Unieke FAQ ID: #1132
Auteur:
Laatst bijgewerkt:2014-06-10 14:47