Seven steps to secure ntp servers from DDoS attacks

Seven steps to secure ntp servers from DDoS attacks

Network time protocol (ntp) servers are regularly being used to reflect and amplify spoofed UDP packets towards the target of a DDoS attack. Attacks are growing in size and frequency and sometimes even cause issues for the organisations hosting the reflectors. Servers offering the 'monlist' command are particularly troublesome and can provide a huge amplification affect.

Securing ntp servers on your network not only stops you from becoming involved in an attack on another network, but also saves you from the costs and interruptions to service that the attack may cause on your own infrastructure.

1. To locate any ntp servers on your networks that respond to the monlist command. http://openntpproject.org/ [1] surveys the Internet for ntp servers and is a useful starting point. A script for nmap [2]may give you a more thorough look at the current state of your network. An individual server can be tested with the following commands:

   ```
   $ ntpdc -n -c monlist <a.b.c.d>
   ```

   or

   ```
   $ ntpq -c rv <a.b.c.d>
   ```

2. Minimise your exposure by removing or disable any unnecessary ntp servers that you find.
3. If any of the remaining ntp servers can be isolated from the Internet by a firewall, do so. You might be considering blocking all ntp traffic but this can have an impact on legitimate services. Do so carefully.
4. If possible upgrade the software to NTP-4.2.7p26 or later. This version removes the monlist command.
5. In older versions you can add 'disable monitor' to your ntp.conf configuration file.
6. Team Cymru provide secure configuration templates [3] for Cisco IOS, Juniper JUNOS and ntpd.
7. For other systems contact your vendor for advice and support.

If you need any further advice on how to secure your ntp configuration please contact Janet CSIRT. [4]

Display as Single Column?:

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/seven-steps-secure-ntp-servers-ddos-attacks

Links
[1] http://openntpproject.org/
[2] http://nmap.org/nsedoc/scripts/ntp-monlist.html
[3] http://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html
[4] https://community.ja.net/library/janet-services-documentation/contact-csirt