Vulnerability in NTP's Authenticated Broadcast Mode Operation

Vulnerability	DoS in Network Time Protocol (NTP).
Impact	Prevents a genuine broadcast NTP client from synchronizing its clock with a broadcast NTP server.
Mode	Authenticated Broadcast mode.
Vulnerable Softwares	ntpd v4.2.8p10, v4.2.8p11, v4.2.8p12 and v4.2.8p13.

Attack Description:

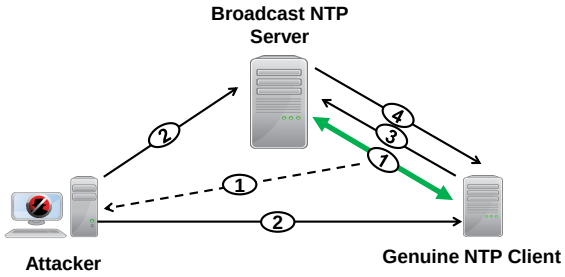

Fig. 1: Steps to Launch the Attack

The steps to launch the attack are shown in Figure 1 and as follows:

1. A genuine broadcast NTP client is first let to successfully synchronize with a broadcast NTP server. In this process, the broadcast server periodically sends broadcast mode 5 packets and as soon as genuine broadcast client receives first mode 5 packet, its NTP daemon sends mode 3 packets to broadcast server to calculate the path propagation delay. After this, genuine client successfully synchronizes its clock with the broadcast NTP server. From this communication between genuine NTP client and broadcast server, a designated attacker intercepts one mode 3 packet and one mode 5 packet.

2. Once attacker captures the required packets, it can launch the attack from anywhere in the wild but at a time T_f such that offset calculated by genuine client at T_f is greater than the panic threshold. To target genuine client, malicious client continuously replays copies of mode 5 and mode 3 query at regular intervals.

3. On receiving copies of mode 5 packet replayed in previous step, NTP daemon of genuine client surprisingly starts sending mode 3 packets to broadcast server to recalculate the path propagation delay.

4. Since broadcast NTP server continuously receives copies of mode 3 NTP packets replayed in Step 2, broadcast server sends Kiss-o'-Death (KoD) packets to genuine NTP client instead of valid mode 4 responses due to which genuine client is not able to calculate the path propagation delay. As a result, genuine client is not able to resynchronize its clock with the broadcast NTP server.

To capture the mode 5 and mode 3 packets in authenticated broadcast mode, attacker must either be a part of same broadcast network or control a slave in that broadcast network which can capture the required packets on attacker's behalf and send it to attacker.