Автор: adm
07.02.14 14:46 -

В январе 2014 года на сайте ntp.org появилось следующее сообщение:

>>-----Цитата---->>

NTP users are strongly urged to take immediate action to ensure that their NTP daemon is not susceptible to use in a reflected denial-of-service (DRDoS) attack. Please see the NTP Security Notice
for more information.

<<-----Цитата----<<>>-----Цитата---->>

Пользователей NTP настоятельно просим незамедлительно убедиться, что их NTP демон не подвержен атаке DRDoS (усиление трафика). См. NTP Security Notice для большей информации.

<<-----Цитата----<<

Несмотря на то, что уязвимость была закрыта еще в 2010 году в версии 4.2.7p26, во многих дистрибутивах до сих пор распространяется версия 4.2.6 или ранее. Пользователям этих версий следует обновиться на версию 4.2.7p26. Если это по каким-то причинам невозможно, следует использовать либо noquery в разрешениях по умолчанию, чтобы отключить все статусные запросы, либо
disable monitor
для отключения только команды
ntpdc -c monlist
, либо ограничить доступ к ntpd настройками файрволла.

Атака DRDoS в данном случае использует то, что демон ntpd работает по протоколу UDP, а также то, что пакет ответа на команды REQ_MON_GETLIST и REQ_MON_GETLIST_1 содержит в 3600~5500 раз больше данных, чем пакет запроса. Таким образом, если подделать IP адрес отправителя запроса на IP-адрес жертвы, то ей придет огромный трафик ответов от NTP сервера, забивая входящий канал мусором.

ddos , ntp , ntpd

**Read more** http://feedproxy.google.com/~r/org/LOR/~3/UCWg21aDydE/10151385