CERT-UA

Рекомендації
26 листопада 2014

CUA-14-05A
Рекомендації CERT-UA для усунення вразливостей, пов’язаних з некоректним налаштуванням NTP-серверів

Державна служба спеціального зв’язку та захисту інформації України
Державний центр захисту інформаційно-телекомунікаційних систем
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

ЗМІСТ

1. Загальна інформація 3

1.1 Інформація про сервіс NTP 3

1.2 Типові вразливості NTP-серверів 3

2. Рекомендації 5

2.1 Перевірка NTP-серверу предмет некоректного налаштування 5

2.2 Рекомендації щодо коректного налаштування сервісу 6

1. Загальна інформація

1.1 Інформація про сервіс NTP

Мережевий протокол часу (англ. Network Time Protocol) — мережевий протокол синхронізації внутрішнього годинника електронно-обчислювальної машини (ЕОМ) з використанням мереж зі змінною латентністю, заснований на комутації пакетів [1].

Докладна реалізація протоколу й системи в цілому описана в:

- RFC 778
- RFC 891
- RFC 956
- RFC 958
- RFC 1305
- RFC 2030
- RFC 4330
- RFC 5905

NTP не слід плутати з daytime protocol RFC 867 або time protocol RFC 868.

1.2 Типові вразливості NTP-серверів

Останнім часом почастішали випадки проведення DDoS-атак, до здійснення яких залучаються не уражені шкідливими програмами комп'ютери (боти), а, натомість, серверне обладнання з некоректно налаштованим програмним забезпеченням [2].

На поточний час зловмисники активно використовують вразливості в конфігурації **ntpd** – програмному забезпеченні, яке забезпечує обслуговування та синхронізацію системного часу. Вразливість, має ідентифікатор в системі CVE (CVE-2013-5211) [3].

Механізм DDoS-атаки, заснований на згаданій вразливості ntpd, полягає у генеруванні зловмисником специфічних запитів (GET_MONLIST) до NTP-серверів із підміною дійсної IP-адреси джерела запиту IP-адресою жертви атаки. В свою чергу, некоректно налаштовані NTP-сервери у відповідь на такі запити відправляють відповідь, що містить інформацію про 600 останніх клієнтів серверу часу (тих, що відправляли запити до цього NTP-серверу). При такому «інформаційному обміні» кожен запит до NTP-серверу примушує його генерувати відповідь, розмір якої більший у десятки разів від розміру запиту. Коефіцієнт підсилення (з англ. – «amplification») у такому разі складає близько 40-50 разів.

Крім того, зважаючи на використання програмним забезпеченням ntpd протоколу UDP, встановлювати з’єднання не є необхідним (stateless protocol), тому підміна IP-адреси джерела запиту є можливою.

2. Рекомендації

2.1 Перевірка NTP-серверу предмет некоректного налаштування

Для перевірки наявності вразливості серверу до атак можна виконати наступний запит в linux-подібній ОС [2]:

ntpdc -n -c monlist <IP-адреса серверу>

Якщо сервер вразливий, то буде отримано відповідь з інформацією щодо 600 останніх клієнтів NTP-серверу. Приклад відповіді вразливого серверу зображено на рис. 1.

```
cert@db:~$ ntpdc -n -c monlist 193.109.[redacted]
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
193.29.204.26          47449 193.109.249.205        4 7 2      0   9600       0
194.28.88.2               80 193.109.249.205    62017 7 2      0      0       0
193.109.248.2            123 193.109.249.205     4684 4 4      0   1024     277
192.168.10.231           123 192.168.1.1         6630 3 1      0    719     534
119.252.190.207         2312 193.109.249.205       90 7 2      0      0     545
192.168.0.199            123 192.168.1.1         5895 3 4      0   1024     659
69.31.20.78               80 193.109.249.205     3295 7 2      0    769    2607
103.4.19.206              21 193.109.249.205    45984 7 2      0    153    2691
184.105.139.116        44745 193.109.249.205        1 6 2      0      0    5813
37.48.89.3                80 193.109.249.205      816 7 2      0      2   11632
95.211.202.193            80 193.109.249.205     3227 7 2      0      2   11632
```

Рис. 1

В разі, якщо сервер не вразливий до подібного роду атак, то буде отримано відповідь, яка зображено на рис.2.

```
pc@HP-ENVY:~$ ntpdc -n -c monlist 91.226.136.136
91.226.136.136: timed out, nothing received
***Request timed out
pc@HP-ENVY:~$
```

Рис. 2

2.2 Рекомендації щодо коректного налаштування сервісу

Використовуйте оновлення

Оновити версію ntpd до 4.2.7p26 та вище. Версії до 4.2.6.x включно містять перераховані в п.1 вразливості.

Відключення monlist

Для відключення функції monlist додайте у конфігураційному файлі ntp.conf запис «disable monitor».

Відключити запити стану сервера

У конфігураційному файлі ntp.conf додати такі записи:

restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

Обмеження доступу

Є можливість обмежити доступ до NTP-серверу в межах локальної мережі, або дозволити доступ тільки окремим хостам. Для цього у конфігураційному файлі ntp.conf додайте такі записи [4]:

Restrict default noquery
restrict localhost
restrict 192.168.0.0 netmask 255.255.0.0 (IP-адреси локальної мережі)
restrict 192.168.1.27 (IP-адреса окремого хоста)

Приклад безпечного налаштування NTP можливо отримати за посиланнями:

- http://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html
- https://www.freebsd.org/doc/ru/books/handbook/network-ntp.html

3. Корисні посилання

[1] https://en.wikipedia.org/wiki/Network_Time_Protocol

[2] http://cert.gov.ua/?p=1396

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5211

[4] http://www.kb.cert.org/vuls/id/348126

[5] http://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html

[6] https://www.freebsd.org/doc/ru/books/handbook/network-ntp.html

Зміни до документу

- 26.11.2014: Перший випуск.