NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Saugos biuletenis

TLP:GREEN

2015-04-14

Nacionalinis kibernetinio saugumo centras, praneša, kad plačiu mastu vykdomos paslaugų trikdymo atakos (angl. *„PingBack DDoS“*), pasinaudojant turinio valdymo sistemos „Wordpress“ pažeidžiamumu (angl. *„Wordpress exploit“*).

Tikslesnė informacija administratoriams:

Išnaudojant pasauliniame interneto tinkle esančių interneto svetainių turinio valdymo sistemos „Wordpress“ saugumo spragas atakuotojai gali siūsti POST (angl. *„PingBack”*) užklausas į kitus tinklapius. Atakos metu interneto svetainės įvykių žurnalo ištraukoje gali būti matoma panaši informacija:

64.201.171.14 - - [12/Apr/2016:12:32:09 +0300] "GET /lt HTTP/1.0" 200 3185 "-" "WordPress/4.1.10; http://www.swd.ca; verifying pingback from 185.130.6.100"
180.92.128.251 - - [12/Apr/2016:12:32:08 +0300] "GET /lt HTTP/1.0" 200 3185 "-" "WordPress/4.1.10; http://fiberlink.net.pk; verifying pingback from 185.130.6.100"
46.105.58.215 - - [12/Apr/2016:12:32:08 +0300] "GET /lt HTTP/1.0" 200 3185 "-" "WordPress/3.9.3; http://www.kolor.com; verifying pingback from 185.130.6.100"\

Siekiant užtikrinti svetainės tinkamą apsaugą nuo galimų DDoS atakų, būtina patikrinti svetainės sisteminius įrašus (įvykių žurnalą). Nustačius, kad vykdoma „PingBack“ tipo ataka, rekomenduojame užsirašyti, kokį „user-agent“ vardą naudoja piktavaliai. Serveriuose su „Apache“ programine įranga atakos blokavimui pagal „user-agent“ parametrą, galima panaudoti pridedamą „.htaccess“ bylos kodą:

```
$ cat .htaccess
< IfModule mod_rewrite.c>
  RewriteEngine On
  RewriteCond %{HTTP_USER_AGENT} ^WordPress [NC]
  RewriteRule .* - [F,L]
< /IfModule>
```

Varnelė ^ prie „user-agent“ (pvz., „^WordPress“) nurodo, kad bus blokuojamos visos užklausos iš šio „user-agent“.

Konkrečios atakos atveju gali būti naudojama kitas „user-agent“ vardas (vietoje „WordPress“ kitas vardas: „ApacheBench“). Galima blokuoti keletą „user-agent“ vardų, pvz. WordPress ir ApacheBench:

```
$ cat .htaccess
< IfModule mod_rewrite.c>
  RewriteEngine On
  RewriteCond %{HTTP_USER_AGENT} ^(WordPress|ApacheBench) [NC]
  RewriteRule .* - [F,L]
< /IfModule>
```

Biuletenis parengtas remiantis VĮ „Infostruktūra“ rekomendacija.

Šaltiniai:

1. **https://isc.sans.edu/forums/diary/Wordpress+Pingback+DDoS+Attacks/17801**
2. **https://ma.ttias.be/block-user-agent-in-htaccess-for-apache-webserver/**

Nacionalinis kibernetinio saugumo centras
Kibernetinio saugumo ir telekomunikacijų tarnyba
prie Krašto apsaugos ministerijos
Šilo g. 5A, LT-10322 Vilnius,
Tel. +370 5 210 3849, www.nksc.lt, el. p. info@nksc.lt