Shellshock - nastavak priče

Čini se da prve zakrpe za ***Shellshock*** napad nisu u stanju pružiti punu zaštitu. Nakon što je objavljena ranjivost CVE-2014-6271 [1], a zatim i zakrpana verzija *basha*, istraživači su našli nove propuste, koji su prijavljeni kao CVE-2014-7169 [2], CVE-2014-7186 [3] i CVE-2014-7187 [4]. Stoga se ubrzano pojavljuju još novije verzije paketa ***bash*** koje rješavaju sve navedene ranjivosti.

Objavljen je kod kojim možete testirati da li je vaša verzija *basha* sigurna.

```
env 'x=() { :;}; echo vulnerable' 'BASH_FUNC_x()=() { :;}; echo vulnerable' bash -c "
echo test"
```

Ako je rezultat ovakav (ili sličan), otvoreni ste za *shellshock* napad:

```
$ env 'x=() { :;}; echo vulnerable' 'BASH_FUNC_x()=() { :;}; echo vulnerable' bash -c
 "echo test"
vulnerable
bash: BASH_FUNC_x(): line 0: syntax error near unexpected token `)'
bash: BASH_FUNC_x(): line 0: `BASH_FUNC_x() () { :;}; echo vulnerable'
bash: error importing function definition for `BASH_FUNC_x'
test
```

Ako je rezultat ovakav:

```
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
bash: error importing function definition for `BASH_FUNC_x()'
test
```

tada je prva verzija *shellshock* napada zakrpana, ali ste još uvijek ranjivi. Ono što želite vidjeti je:

```
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `BASH_FUNC_x'
test
```

I još jedan test, koji bi trebao dokazati da niste ranjivi na CVE-2014-7169:

```
cd /tmp; rm -f /tmp/echo; env 'x=() { (a)=>\' bash -c "echo date"; cat /tmp/echo
```

Ako vidite ovakav rezultat:

```
bash: x: line 1: syntax error near unexpected token `='
bash: x: line 1: `'
bash: error importing function definition for `x'
Fri Sep 26 11:49:58 GMT 2014
```

gdje je u zadnjem retku ispisan datum, vaš je sustav još uvijek ranjiv. Sigurni smo ako piše:

```
date
cat: /tmp/echo: No such file or directory
```

Rezultat može varirati na različitim distribucijama Linuxa.

Na Mreži se razvila rasprava o tome da li su i Macovi ranjivi na shellshock napad? Kao što znamo, Apple koristi Unixovu jezgru. Apple je izdao prigodnu izjavu koju je sročio njihov PR: OS X je siguran "by default" jer korisnici nisu izloženi napadima ukoliko nisu konfigurirali napredne Unix servise. Veseljaci su to okrenulu na šalu: Korisnici Maca su sigurni jer su nisu dovoljno pametni da bi koristili napredne funkcionalnosti. No nećemo se vrijeđati, Apple izjavljuje da ubrzano rade na ispravcima, kako ni napredni korisnici ne bi bili ugroženi.

Kvaka je u tome da su s nezakrpanim *bashom* ugroženi svi sustavi koji pružaju servise koji pozivaju ljusku, među njima na primjer HTTPD i DHCP.

Metasploit, poznati penetracijski alat, dobio je ***Shellshock modul***, pa možemo očekivati povećan broj pokušaja napada na servere. Pobrinite se da ne postanete žrtva.

ned, 2014-09-28 17:38 - Aco Dmitrović**Vijesti:** Sigurnost [5]
Kategorije: Operacijski sustavi [6]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1436

Links
[1] http://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAA&url=http%3A%2F%2Fweb.nvd.nist.gov%2Fview%2Fvuln%2Fdetail%3FvulnId%3DCVE-2014-6271&ei=CywoVN3ROpLaaOvggfgN&usg=AFQjCNGryFJeKgO9-y-K0QNQWipEiVDSOQ&bvm=bv.76247554,d.d2s
[2] http://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCEQFjAB&url=http%3A%2F%2Fweb.nvd.nist.gov%2Fview%2Fvuln%2Fdetail%3FvulnId%3DCVE-2014-7169&ei=USwoVLmEO4-WapK5goAN&usg=AFQjCNE2FDTYqRu6PFSTSa8-Gf-kNojqnw&bvm=bv.76247554,d.d2s
[3] https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0CC0QFjAD&url=https%3A%2F%2Fcve.mitre.org%2Fcgi-bin%2Fcvename.cgi%3Fname%3DCVE-2014-7186&ei=cCwoVIDtGM3qaqSBgdgI&usg=AFQjCNGM9DsI4MnZWK12E5PjmjeaPPPwAw&bvm=bv.76247554,d.d2s
[4] http://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0CC0QFjAD&url=http%3A%2F%2Fweb.nvd.nist.gov%2Fview%2Fvuln%2Fdetail%3FvulnId%3DCVE-2014-7187&ei=miwoVISIEMrtaKPEgOgE&usg=AFQjCNEScjzdFgIYrxOapOPCp2qg7pl01Q&bvm=bv.76247554,d.d2s
[5] https://sysportal.carnet.hr/taxonomy/term/13
[6] https://sysportal.carnet.hr/taxonomy/term/26