Kritična ranjivost basha omogućava udaljene napade

Pod oznakom CVE-2014-6271 jučer je objavljena ranjivost popularne U*xove ljuske ***bash*** (*Bourne again shell*). NIST je ranjivost ocijenio kritičnom (10/10), što svakako treba pobuditi našu pažnju. Ranjivost pogađa inačice basha od 1.14 do 4.3 i dobila je dva imena: ***Bash Bug*** i ***Shellshock***.

Radi se pogrešci pri obradi varijabli u radnoj memoriji (environment), pri čemu ljuska izvršava kod koji slijedi nakon definicije funkcije. Provjeru ranjivosti obavite s ove dvije naredbe:

```
env X="() { :;} ; echo shellshock" /bin/sh -c "echo completed"

env X="() { :;} ; echo shellshock" `which bash` -c "echo completed"
```

Ako na komandnoj liniji ugledate tekst ***shellshock***, u problemima ste! Ranjivi su svi OS-ovi na koje je prenesen bash, a to mogu biti i Mac-ovi.

Ovdje i nije toliko važno da li je ranjivo vaše osobno (Linux) računalo, već nas treba brinuti mogućnost pozivanja ljuske iz web aplikacija, iz HTML ili CGI koda, što otvara mogućnost udaljenog napada na servere.

Stephane Chazelas, dvadesetdvogodišnjak koji je otkrio ranjivost, pričekao je s njenom objavom dok se ne unesu zakrpe. Rok koji je dao istekao je jučer, a čini se da ga je većina distribucija dobro iskoristila.

No važno je da provjeru obavite na svojim serverima i što prije instalirate novu inačicu paketa. Problema će biti ako još uvijek koristite neko starije izdanje Linuxa, za kojeg se više ne objavljuju sigurnosne zakrpe. U tom slučaju, požurite s dogradnjom na novo izdanje! Ili barem zamijenite bash nekom drugom inačicom ljuske, ako vam je bash zadan kao standard.

čet, 2014-09-25 11:20 - Aco Dmitrović**Vijesti:** Sigurnost [1]
Kategorije: Operacijski sustavi [2]
Vote: 4.5

Vaša ocjena: Nema Average: 4.5 (2 votes)

Source URL: https://sysportal.carnet.hr/node/1435?page=0

Links
[1] https://sysportal.carnet.hr/taxonomy/term/13
[2] https://sysportal.carnet.hr/taxonomy/term/26