Ispravljen ozbiljan propust u jezgri Linuxa

Održavatelji Linuxova kernela ispravili su grešku u funkciji *n_tty_write* koja upravlja pseudo tty terminalom. Radi se o ozbiljnoj grešci koja izaziva korupciju memorije i tako potencijalno omogućava eskalaciju privilegija. Greška je unesena u kod kernela 2.6.31 još 2009. godine i od tada ostavlja ranjivima brojna računala.

Analitičari ističu da se ovako ozbiljni propustu ne pojavljuju tako često. Potencijalno je iskoristiv, ne ovisi o arhitekturi ili konfiguraciji, a ranjiv je cijeli niz kernela, od verzije 2.6.31 pa sve do predzadnje.

Kod za exploit objavljen je na adresi http://bugfuzz.com/stuff/cve-2014-0196-md.c [1], tako da se radoznalci mogu poigrati s njime. Na webu ćete naći komentare scriptie kidza, koji se žale da kod ne radi. Radi se o tome da bi ga trebalo prilagoditi lokalnom sustavu, nakon što se pogleda sadržaj datoteke /proc/kallsyms, gdje se nalaze lokacije varijabli aktivnog kernela. Vlasnik te datoteke je root, ali njen sadržaj mogu pročitati i ostali korisnici, jer svi imaju dozvole za čitanje.

```
$ ls -l /proc/kallsyms
-r--r--r-- 1 root root 0 Svi 27 12:42 /proc/kallsyms
```

Ispravak je već napravljen, možete ga pogledati ovdje [2].

Debian je ubacio ispravak u novu inačicu jezgre, pa samo treba instalirati novi paket i restartati OS.

uto, 2014-05-27 13:10 - Aco Dmitrović**Vijesti:** Sigurnosni propusti [3]
Kategorije: Operacijski sustavi [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1399

Links
[1] http://bugfuzz.com/stuff/cve-2014-0196-md.c
[2] https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4291086b1f081b869c6d79e5b7441633dc3ace00
[3] https://sysportal.carnet.hr/taxonomy/term/14
[4] https://sysportal.carnet.hr/taxonomy/term/26