

Ranjiv loše konfiguriran sftp



SSH je servis bez kojeg je nezamisliv radni dan svakog sistemca. **Secure FTP** dio je istog paketa, omogućava siguran/kriptiran prijenos datoteka. Implementira se na dva načina, kao *sftp-server*, ili kao *in-process* server koji ne zahtijeva dodatnu podršku kada se koristi s **ChrootDirectory**.

Ovako bi nekako trebala izgledati konfiguracija:

```
Subsystem sftp internal-sftp
Match Group sftp
ChrootDirectory %h
ForceCommand internal-sftp
AllowTcpForwarding no
```

Ako korisnike treba pustiti nekamo izvan njihova direktorija, zadajemo to ovako:

```
Subsystem sftp internal-sftp -d /var/www
```

Dodatna zaštita može se postići parametrom `-R` koji korisnicima daje samo *read only* prava, kako ne bi mogli mijenjati sadržaj direktorija u koji su usmjereni.

Ako administrator zaboravi konfigurirati **chroot**, omogućio je korisnicima pristup cijelom filesystemu, pa i `/proc` direktoriju, što se može zloupotrebjavati za različite maštovite napade.

Postoje grafički klijenti koji omogućavaju prijenos datoteka klikanjem, bez zadavanja naredbi na komandnoj liniji. Time je i širem krugu korisnika omogućen pristup dijelovima datotečnog sustava u koje ne bi smjeli zalaziti.

Objavljen je i kod za [proof-of-concept](#) [1], pa se radoznalci mogu poigrati s njime. Time je opasnost još veća. Ranjive su verzije OpenSSH <= 6.6, pa preporučujemo da odmah provjerite konfiguraciju i što prije instalirate OpenSSH 6.7, u kojem je greška ispravljena.

čet, 2014-10-09 11:34 - Aco Dmitrović **Vijesti:** [Sigurnosni propusti](#) [2]

Kategorije: [Servisi](#) [3]

Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

Source URL: <https://sysportal.carnet.hr/node/1439?page=0>

Links

- [1] <http://seclists.org/fulldisclosure/2014/Oct/35>
- [2] <https://sysportal.carnet.hr/taxonomy/term/14>
- [3] <https://sysportal.carnet.hr/taxonomy/term/28>