Sigurnosni propust X11Forwardinga SSH poslužitelja

OpenBSD je objavio sigurnosnu zakrpu za megapopularni OpenSSH kojom se ispravlja propust [1] u čišćenju (sanitiziranju) argumenata xauth *[2]* programa, zaduženog za prikaz i uređivanje podataka o autorizaciji između računala klijenta i poslužitelja. Propust je nastao radi činjenice da OpenSSH nije čistio prosljeđene naredbe, što je napadaču otvorilo mogućnost iskorištavanja poslužitelja čiji *ssh daemon* dozvoljava *X11Forwarding*. Na taj način napadač bi mogao doći do informacija koje mu inače ne bi bile dostupne, srećom na poprilično ograničen način.

Kako i sami autori priznaju, *xauth* nije pisan sa zlim korisnicima na umu (što je, čini se, i u ovom slučaju višegodišnja greška u dizajnu, ali u vrijeme kad je ovaj komad softvera pisan problem malicioznih korisnika uistinu je bio nekoliko magnituda manje), pa ne čisti ulazne naredbe od smeća i potencijalno malicioznog koda.

Srećom, domet ovog sigurnosnog propusta vrlo je ograničen: napadač ostaje na nivou privilegija korisnika pod kim se prijavio na poslužitelj i ograničen je na datoteke u korisnikovom vlasništvu; korištenjem xauth naredbi moguće je saznati nešto više o poslužitelju i potencijalno ugroziti poslužitelj omogućivši klijentu čiji login je /bin/false da se dohvati ljuske (/bin/nologin nije ranjiv).

Rješenje problema je vrlo jednostavno: onemogućenje *X11Forwardinga* u konfiguracijskoj datoteci *ssh daemona*.

Iako se danas relativno rijetko susreće izvan akademske zajednice, korištenje klijenta kao X11 terminala koji samo prikazuje sliku dok glavninu posla obavlja moćan CPU na poslužitelju bilo je dugo vremena uobičajen način komunikacije na Unix računalima. Danas je klijent-poslužitelj arhitektura drugačija i rijetko se susreće potreba za udaljenim pokretanjem grafičke aplikacije, no ta je korisna mogućnost zadržana, iako je isključena. Drugim riječima, OpenSSH dolazi sa X11Forwarding opcijom isključenom, što je odlična zaštita od gore navedenog sigurnosnog propusta.

Neke distribucije Linuxa, međutim, instaliraju se s uključenim X11Forwardingom, na primjer Red Hat – tvrtka koju su autori OpenSSH specifično naveli kao loš primjer. Zato svakako provjerite i isključite je ako vam ta mogućnost nije potrebna.

Ovaj sigurnosni propust srećom nije pretjerano ozbiljan i ne bi trebao otvoriti vrata ozbiljnijim napadima – no standardno upozorenje: "budite ažurni sa sigurnosnim zakrpama" vrijedi i za njega.

sri, 2016-03-23 11:27 - Radoslav Dejanović**Vijesti:** Sigurnost [3]
Kategorije: Servisi [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1627

Links
[1] https://www.exploit-db.com/exploits/39569/
[2] http://www.x.org/archive/X11R6.7.0/doc/xauth.1.html
[3] https://sysportal.carnet.hr/taxonomy/term/13
[4] https://sysportal.carnet.hr/taxonomy/term/28