Ranjivost Linux GLIBC 2.9 biblioteke

Svježe otkriven sigurnosni propust [1] u GLIBC biblioteci verzije 2.9 i novijih tiče se pogreške u funkciji getaddrinfo(), pri čemu se otvara potencijalno opasan vektor koji u krajnosti može dovesti do kompromitiranja računala.

Iskorištavajući propust navedene *glibc* funkcije, maliciozni (ili kompromitirani!) DNS servis može poslati posebno oblikovan maliciozni kod koji će izazvati *buffer overflow* na stogu i omogućiti izvršavanje koda s visokim privilegijama, ovisno o aplikaciji koja je pozvala funkciju.

Propust, naravno, nije moguće izvesti bez DNS poslužitelja sposobnog i voljnog poslati klijentu patološki kod. U načelu to znači da, ako nemate običaj svako toliko mijenjati DNS poslužitelje, relativno ste sigurni. S druge strane stoji činjenica da na višekorisničkom računalu svaki korisnik može samo za sebe promjeniti adresu DNS poslužitelja i tako i bez administratorovog znanja malo otškrinuti vrata malicioznom poslužitelju. Što će se zatim dogoditi ovisi o ovlastima korisnika i programu koji je zatražio usluge getaddrinfo() funkcije: koristi li korisnik ssh ili neku sličnu aplikaciju sa većim privilegijama, eto problema!

Brzo i efikasno rješenje u svakom slučaju jest na vatrozidu zabraniti promet prema bilo kojem drugom DNS poslužitelju osim onog (jednog ili nekoliko njih) u čiju nekompromitiranost vjerujemo.

Konačno rješenje, naravno, jest instalirati sigurnosnu zakrpu za glibc.

Ovaj sigurnosni propust podigao je dosta prašine u specijaliziranim medijima, i to s razlogom: sigurnosni propust je vrlo ozbiljan i svi oni uređaji koji neće dobiti sigurnosnu nadogradnju (ponovo, mnoštvo embedded i IoT uređaja koji pogone ovu ili onu verziju Linux distribucije) ostat će ranjivi na ovaj propust. Sreća u nesreći je što većina njih najčešće komunicira s DNS poslužiteljem lokalnog routera ili ISP-a, čime se ovaj propust malo ublažava, iako svakako ne u potpunosti uklanja. Imate li priliku kontrolirati vatrozid između tih uređaja i Interneta, možete značajno smanjiti opasnost postavljanjem odgovarajućih zabrana prometa kao i u gore navedenom slučaju.

Android, Google tvrdi, nije osjetljiv na ovaj propust jer koristi svoju inkarnaciju glibc biblioteke - Bionic.

Primjer skripte koja postavlja pravila vatrozida za korištenje točno određenih DNS poslužitelja (podrazumjevano stanje prometa je DENY ili DROP):

```
#!/bin/bash
DNS_SERVER="<ip adresa prvog DNS-a> <ip adresa drugog DNS-a>..."

for ip in $DNS_SERVER
do
   /sbin/iptables -A OUTPUT -p udp -d $ip --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
   /sbin/iptables -A INPUT -p udp -s $ip --sport 53 -m state --state ESTABLISHED -j ACCEPT
   /sbin/iptables -A OUTPUT -p tcp -d $ip --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
   /sbin/iptables -A INPUT -p tcp -s $ip --sport 53 -m state --state ESTABLISHED -j ACCEPT
done
```

čet, 2016-02-18 10:38 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [2]

Kategorije: Servisi [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/1614

Links
[1] https://googleonlinesecurity.blogspot.hr/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html
[2] https://sysportal.carnet.hr./taxonomy/term/14
[3] https://sysportal.carnet.hr./taxonomy/term/28