

BIND: kako sakriti inačicu DNS poslužitelja?



Ukoliko ste ikad rabili CARNetovu uslugu provjere ranjivosti vaše mreže, vrlo vjerojatno ste dobili uputu da bi bilo dobro sakriti inačicu BIND-a. Ova operacija se provodi u svrhu povećane sigurnosti, jer eventualni napadač nema informaciju o kojoj se točno inačici softvera radi.

Samim tim prvo mora saznati tu informaciju, ili napadati na slijepo, što mu oduzima više vremena. Ako zna točnu informaciju o inačici, napadač može upotrijebiti već gotove alate za provaljivanje, a za to ne mora imati nikakva posebna znanja (tzv. "script kiddies").

Informaciju o inačici BIND-a možete saznati na više načina:

```
# nslookup -q=txt -class=CHAOS version.bind DNS_SERVER
```

DNS_SERVER je adresa poslužitelja čiju inačicu želite saznati:

```
# nslookup -q=txt -class=CHAOS version.bind dns.carnet.hr
Server:          dns.carnet.hr
Address:         161.53.123.3#53
version.bind    text = "9.2.4"
```

Drugi način je preko alata dig:

```
# dig @dns.carnet.hr version.bind chaos txt
; <<>> DiG 9.2.4 <<>> @dns.carnet.hr version.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48683
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;version.bind.                CH      TXT
;; ANSWER SECTION:
version.bind.                 0      CH      TXT      "9.2.4"
```

U svakom slučaju, inačica poslužitelja je upisana u zapisu "version.bind".

Moramo spomenuti da ova informacija napadaču nije od presudne važnosti ukoliko je vaš sustav redovito održavan i patchiran, jer onda napadač nema ulazni vektor. No, ukoliko želite, vrlo lako možete sakriti tu informaciju. Dovoljno će biti u datoteci named.conf upisati opciju:

```
version "No version";
```

To morate napraviti u bloku "options", pa će izmjena izgledati otprilike ovako:

```
options {
```

```
directory "/var/cache/bind";
// forwarders {
//     0.0.0.0;
// };
allow-transfer { 161.53.XXX.YY; 161.53.ZZZ.ZZ; };
auth-nxdomain no;    # conform to RFC1035
version "No version";
};
```

te napraviti

```
# rndc reload
```

Provjerite postoje li kakve poruke o greškama u log datoteci /var/log/daemon.log. Sad bi DNS poslužitelj na upit o inačici trebao odgovarati ovako:

```
$ nslookup -q=txt -class=CHAOS version.bind www.test.hr
Server:          www.test.hr
Address:         193.198.X.3#53
version.bind     text = "No version"
```

Čestitamo, upravo ste dodali jedan mali dodatak sigurnosti vašeg poslužitelja.

- [Logirajte](#) [1] se za dodavanje komentara

pet, 2007-06-15 16:19 - Željko Boroš**Kuharice**: [Linux](#) [2]
[Za sistemce](#) [3]
Kategorije: [Servisi](#) [4]
Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/230>

Links

[1] <https://sysportal.carnet.hr/sysportallogin>
[2] <https://sysportal.carnet.hr/taxonomy/term/17>
[3] <https://sysportal.carnet.hr/taxonomy/term/22>
[4] <https://sysportal.carnet.hr/taxonomy/term/28>