```
rate-limit {
responses-per-second 5;
log-only yes;
};
};
```

KNOT DNS

V případě KNOT DNS je RRL dostupný jako standard od verze 1.2.0-RC3. I v tomto případě není RRL ve výchozím nastavení zapnutý a je nutné jej v systémové sekci nastavit na hodnotu enabled. Každá hodnota větší než 0 znamená počet odpovědí za sekundu (např. rate-limit 50 znamená 50 odpovědí za sekundu).

Od verze 1.2.0 je možné také nastavit tzv. SLIP interval. Hodnota, kterou u rate-limit-slip nastavíme, definuje, jakým způsobem se bude server chovat k paketům, které nevyhoví nastavení v položce rate-limit.

Pokud nastavíme hodnotu rate-limit-slip například na 2, na každý druhý zablokovaný dotaz odpoví server truncated. Doporučená hodnota 1 má tu výhodu, že amplifikaci omezí a zároveň žádný dotaz neignoruje.

NSD

Produkt NSD má od verze 3.2.15 podobně jako ostatní autoritativní servery implementovaný Response Rate Limiting. V NSD3 a NSD4 je potřeba RRL povolit pomocí -enable-ratelimit. Podobně jako v případě serveru KNOT DNS je možné nastavit také hodnotu RRL SLIP. Defaultně je tato hodnota nastavená na 2.

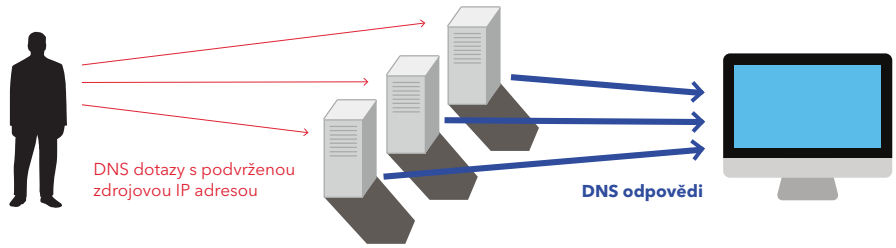
Vhodné nastavení je závislé na různých faktorech a je třeba porovnat vaši konkrétní situaci s manuálem NSD. V souboru nsd.conf je také možné podle potřeby nastavit hodnoty rrl-size, rrl-ratelimit, rrl-whitelist-ratelimit či rrl-whitelist.

NTP amplification attack

NTP (Network Time Protocol) představuje protokol pocházející z rodiny protokolů TCP/IP, který slouží k synchronizaci času na počítačích a dalších zařízeních v síti. NTP využívá UDP protokol (User Datagram Protocol), a proto může podobně jako DNS umožnit vykonání úspěšného DDoS útoku.

V případě NTP amplification zašle útočník NTP serveru požadavek s podvrženou zdrojovou IP adresou, která je zároveň adresou zamýšlené oběti. Server nedokáže posoudit, zda dotaz přišel od legitimního uživatele, a proto na něj odpoví. V odpovědi se pak projeví i „amplification“, tedy zesílení či zvětšení, protože odpověď, kterou server zašle, je násobně větší než přijatý dotaz. Princip je tedy zcela stejný jako v případě DNS, jen použitý aplikační protokol je jiný.

Jeden z příkazů používaných v rámci NTP je monlist, který slouží k monitorování provozu na serveru. Pokud je server zranitelný, pak pomocí příkazu monlist lze získat seznam posledních šesti set IP adres, které se k němu připojily.



Princip DNS amplification útoku

Zda je zranitelný, lze otestovat pomocí příkazu `ntpdc -n -c monlist IP`, kde IP znamená IP adresu serveru, na který se dotazujete. Pokud od serveru obdržíte odpověď, pak to znamená, že tento server se může zneužít k amplification útoku.

Obrana

Pokud provozujete NTP server, je možným způsobem ochrany před jeho zneužitím upgrade na verzi 4.2.7p26, případně vyšší, neboť v těchto variantách je příkaz monlist zcela odstraněn. Protože však jde o vývojové verze, doporučuje se spíše změna konfigurace existujícího softwaru.

Ta spočívá v nastavení hodnoty monlist na disabled, což je možné udělat v souboru /etc/ntp.conf přidáním direktivy „noquery“ do řádků „restrict default“. Konkrétně jde o tyto dva řádky:

```
restrict default kod nomodify notrap nopeer
noquery
restrict -6 default kod nomodify notrap nopeer
noquery
```

Toto nastavení samozřejmě platí i pro veřejné NTP servery. Je také potřeba pamatovat na to, že se tento problém netýká pouze linuxových/unixových systémů, ale také dalších zařízení, jako jsou routery Cisco či Juniper. Celá zranitelnost se popsala v CVE-2013-5211.

SNMP amplification attack

Simple Network Management Protocol (SNMP) je internetový protokol, který se používá na sběr statistik, testování stavu zařízení a případný aktivní management síťových zařízení a serverů. Nejčastěji jde o routery, switche, servery, racky a podobně.

SNMP pracuje stejně jako DNS a NTP na UDP protokolu. Na jedné straně komunikace je monitorující zařízení, tzv. SNMP manager, na druhé straně jsou pak monitorovaná zařízení, tzv. SNMP agenti. SNMP pak umožňuje administrátorům sledovat z jednoho místa stav všech síťových zařízení.

Útočník může opět podvrhnout zdrojovou IP adresu v hlavičce paketu, v tomto případě nesoucího požadavek SNMP GET. Takto zaslaný SNMP dotaz se bude koncovému zařízení jevit jako legitimní a odpověď se zašle na podvrženou IP adresu patřící oběti.

V tomto případě je potřeba určit, která zařízení by měla SNMP podporovat a na kterých to naopak není třeba. Pokud jde o přístroje, u nichž se SNMP nevyužívá, je vhodné u nich SNMP vypnout.

V případě, kdy je podpora SNMP nezbytná, je nejlepší přejít na SNMPv3, který vyžaduje ověření prostřednictvím jména a hesla a zároveň používá šifrované spojení. Community strings, které slouží jako uživatelské jméno a heslo pro přístup ke statistikám v zařízení, se podporují pouze ve verzi 1 a 2. Pokud se rozhodnete přejít na variantu 3, nezapomeňte na vašich zařízeních starší verze zakázat.

Velkou výhodou varianty 3 oproti předchozím verzím je také možnost šifrovaného přenosu informací.

Pokud se ale z nějakého důvodu rozhodnete zůstat u verzí 1 a 2, přesvědčte se, že community strings nejsou veřejně dostupné, a to ani v read-only souboru.

Jestliže SNMP používáte, je také vhodné zabezpečit přístup pomocí ACL (Access Control List). Omezením přístupu jen na určitý počet IP adres, které jsou ve vaší správě, zamezíte tomu, aby váš server odpovídal na dotazy třetích stran, a mohl se tak zneužít k amplification útoku. Monitorování pomocí SNMP může navíc útočník využít také k získávání informací o zařízeních ve vaší síti.

Správnou implementací ACL tak ochráníte vaši síť nejen proti tomu, aby se útoku zúčastnila, ale také proti tomu, aby se stala jeho terčem.

Příště se zaměříme na nevyžádanou poštu a zneužívání cizích doménových jmen k jejímu odesílání. Můžete se tedy těšit na povídání o SPF/DKIM. ■

Autorka pracuje jako specialistka počítačové bezpečnosti ve sdružení CZ.NIC a je členkou národního bezpečnostního týmu CSIRT.CZ.