Zatočte s amplification ataky

Zabezpečení provozovaných systémů a sítí se stává stále důležitější složkou pracovní náplně administrátorů ve všech společnostech. Zdaleka už ale nestačí jen vědět, jak správně nakonfigurovat spravované služby, ale také jak je nejlépe chránit.

ZUZANA DURAČINSKÁ

Důležité je pamatovat nejen na bezpečnost našich vlastních aplikací a dat, ale mít i na paměti, že v propojeném prostředí internetu se mohou provozované služby zneužít také k útokům na jiné uživatele.

Přinášíme vám ve spolupráci s týmem CSIRT.CZ a jeho stejnojmenným webem postupy a návody, které administrátorům pomohou vyřešit nejčastější problémy dříve, než budou zneužity případným útočníkem. Doufáme, že tento seriál věnovaný bezpečnosti síťových služeb pomůže k dalšímu zlepšení na poli bezpečnosti sítí.

V prvním dílu seriálu se společně podíváme na problematiku tzv. amplification útoků.

Amplification útoky obecně

Jak už slovo amplification (česky zesílení) napovídá, jde o útok, při kterém dochází k zesílení konaného útoku prostřednictvím špatně zabezpečené síťové služby.

Pro podobný atak jsou nejvhodnější služby, u kterých lze pomocí relativně malého dotazu vyvolat i několikanásobně větší odpověď.

Útočník musí mít zároveň možnost podvrhnout zdrojovou IP adresu zasílaného požadavku. Podvržením zdrojové IP zajistí, že se odpověď serveru doručí na IP adresu zamýšlené oběti. To je také důvod, proč se při těchto útocích zneužívají služby využívající při komunikaci protokol UDP (User Datagram Protocol).

UDP je protokol nespojovaný, což znamená, že na začátku komunikace klient-server neprobíhá trojcestný „handshake“, který je známý z protokolu TCP. V případě UDP se tedy data z klientské aplikace posílají rovnou serverové části aplikace, a to bez jakékoliv předchozí komunikace.

Také doručení paketů se vzájemně neověřuje a případnou ztrátu paketů tak musí řešit přímo samotná aplikace, například jejich dalším odesláním po vypršení časového limitu.

Tyto skutečnosti pak umožňují útočníkovi nastavit falešnou zdrojovou IP adresu, která se díky absenci jakékoliv kontroly považuje serverem za skutečného žadatele o příslušná data. Pokud jsou pak tato data násobně větší než samotná žádost o jejich poskytnutí, pak má oběť, reprezentovaná falešnou zdrojovou IP adresou, „zaděláno na pořádný problém“.

Doporučení BCP38

Již několik let je známý mechanismus umožňující na úrovni sítí předcházet podobným manipulacím se síťovým provozem, jako se popsaly výše.

Zde máme samozřejmě na mysli ochranu proti spoofingu, kterou popisuje doporučení IETF (Internet Engineering Task Force) BCP38. Toto doporučení se však stále běžně nedodržuje, a pokud se nenasadí plošně, těžko může podobným útokům zabránit.

BCP38 definuje mechanismy pro filtrování odchozích IP adres, tzv. ingress filtering, které mají zabránit tomu, aby bylo možné z konkrétní sítě odesílat pakety, které mají zdrojovou adresu nepatřící do dané sítě.

Pokud by došlo k plošnému nasazení tohoto doporučení, eliminovaly by se ataky závislé na podvržení zdrojové IP adresy. Prvním krokem, jak zabránit zneužití vlastní sítě, je tedy nepochybně implementace BCP38.

Pojďme se blíže věnovat „amplifikátorům“, se kterými se v poslední době nejčastěji setkáváme.

DNS amplification attack

Domain Name Server amplification attack se postupně stal velmi rozšířeným způsobem útoku, a proto je potřeba věnovat zabezpečení DNS serverů zvýšenou pozornost.

V průběhu DNS amplification útoku se zasílají DNS dotazy z podvržené IP adresy, která je stejně jako u ostatních amplification útoků zároveň IP adresou oběti.

Při zpracování DNS dotazů dochází v podstatě k pákovému efektu, při němž útočník posílá DNS serverům malé DNS dotazy, avšak na IP adresu oběti se posílají několikanásobně větší odpovědi. Díky tomuto efektu může i útočník s pomalejší linkou pohodlně zahltit rychlejší internetové připojení vybrané oběti.

Otevřené resolvery

K DNS amplification útoku se často používají rekurzivní name servery. Otevřené resolvery jsou rekurzivní DNS servery, které nemají omezené poskytování DNS služby pouze na zařízení v dané síti.

Z pohledu útočníka mají především tu výhodu, že není při útoku omezen na určitou skupinu doménových jmen, ale může si vybrat, případně i sám připravit DNS záznam, který bude útok co nejvíce zesilovat.

Pokud tedy rekurzivní DNS resolvery ve svých sítích využíváte, je nejlepší, když omezíte odpovědi na dotazy pouze pro IP rozsahy z vaší sítě. Pokud máte v podniku přidělený IP rozsah například 2.2.2.0/24 (tj., 2.2.2.0-2.2.2.255), pak by měl váš rekurzivní DNS server odpovídat pouze na dotazy, které přicházejí z tohoto rozsahu.

Dotazy můžete filtrovat přes ACL (Access Control List), který bude obsahovat jen rozsahy vašich klientů. Jakmile by dotaz přišel z jiné adresy, než je uvedená v ACL, například z 3.3.3.3., neměl by odpověď získat.

Provozování otevřeného resolveru má také další nevýhody, neboť dotazy od cizích zařízení zbytečně spotřebovávají vaše zdroje a útočník může také otrávit cache na resolveru, což představuje pro organizaci bezpečnostní riziko.

Pokud potřebujete, aby váš rekurzivní DNS server odpovídal také na vnější dotazy, či jestliže provozujete autoritativní name servery, je nezbytné vytvořit dobrou politiku limitování dotazů. Autoritativní name servery, které jsou z principu vždy otevřené, by však nikdy neměly zároveň sloužit jako rekurzivní DNS pro klienty ve vaší síti.

Technika RRL (Response Rate Limiting) umožní legitimním uživatelům dotazovat se serveru, ale zároveň omezí dopady případného DNS amplification útoku. V současnosti je implementovaná podpora pro RRL u řady autoritativních serverů.

BIND

V případě BIND se RRL podporuje od verze 9.9.4. Pokud si BIND konfigurujete sami, je třeba použít konfigurační switch. RRL zapnete pomocí příkazu `$./configure –enable-rrl`.

Pokud máte BIND z distribučních balíčků, ověřte si v balíčku changelogu, zda podporuje RRL.

Dále je nutné RRL nastavit v konfiguraci daemona BIND.

Například:

```
options {
directory „/var/named“;
```