DNS resolvery opravují chybu KeyTrap: příliš mnoho klíčů, resolverova smrt

Autor: Depositphotos
Dvě nové zranitelnosti umožňují zahltit DNS resolver a zastavit jeho běžné fungování. Vývojáři totiž neposlouchaly rady tvůrců DNS a jejich doporučení. Silná komunita naštěstí dokázala problém vyřešit.

Zveřejnili jsme BIND ve verzích 9.16.48, 9.18.24 a 9.19.21. Tato vydání zmírňují dopady několika zranitelností, které jsou popsány v našem oznámení. Dvě z těchto zranitelností se týkaly **více implementací** a celého systému DNS:

ISC děkuje Eliasi Heftrigovi, Haye Schulmannové, Niklasi Vogelovi a Michaelu Waidnerovi z německého Národního výzkumného centra pro aplikovanou kybernetickou bezpečnost ATHENE za zodpovědné oznámení zranitelnost KeyTrap a koordinaci jejího odhalení. Výzkumný tým nám také poskytl neocenitelnou pomoc při testování oprav.

V obou případech se jedná o způsoby, kterými může útočník zneužít standardní protokol DNSSEC určený k zajištění integrity DNS a extrémně vytíží prostředky resolveru, což v důsledku způsobí odepření služby legitimním uživatelům.

Co je zranitelnost KeyTrap?

Útočník v podstatě vytvoří zónu DNS s mnoha záznamy DNSKEY a RRSIG a validátor DNSSEC splňující standardy vyzkouší všechny možné **kombinace** těchto záznamů v bláhové naději, že najde jedinou správnou variantu, která bude vyhovovat a bude úspěšně validována.

Pokud validátor neimplementuje explicitní **omezení** množství práce, kterou je ochoten provést, může vynaložit neuvěřitelné množství prostředků na zbytečné zpracování takto připravených dat. Tento útok je patří mezi útoky asymetrické – útočník vynakládá relativně málo úsilí, aby přiměl validátor vynaložit mnohem více úsilí při zpracování zadaného úkolu.

Útok KeyTrap je mimořádně účinný proti starším verzím systému BIND, protože ověřování DNSSEC se historicky provádělo ve stejném vlákně, jako v podstatě všechno ostatní. Tento nedostatek v návrhu serveru BIND, spolu s chybějícím omezením na spotřebu zdrojů při ověřování, umožňovala útočníkovi **zablokovat** zpracování dotazů v resolveru na opravdu dlouhou dobu. Šlo řádově o minuty až hodiny na pomalém procesoru.

Zmírnění dopadů útoku KeyTrap v BIND

Pro zmírnění zranitelnosti KeyTrap jsme v DNS serveru BIND provedli dvě významné změny:

1. BIND nyní omezuje množství práce vynaložené na ověření jedné odpovědi DNSSEC.
2. BIND nyní přenáší ověřování DNSSEC do samostatných vláken.

Druhá změna zajišťuje ochranu i proti dosud neznámým útokům: ověřování DNSSEC již **neblokuje** zpracování jiných požadavků. Díky této změně návrhu serveru BIND nebudou mít KeyTrap a další podobné zranitelnosti související s DNSSEC tak silný dopad na vyřizování ostatních nesouvisejících dotazů. Úprava také zlepšuje odolnost resolveru při útocích pomocí náhodných dotazů zaměřených na domény podepsané protokolem DNSSEC.

Díky těmto změnám bude i útok využívající ověřování DNSSEC, který obejde všechna ostatní omezení, spotřebovat jen zhruba **polovinu** kapacity procesoru na postiženém počítači a druhá polovina zůstane na běžné zpracování legitimních dotazů.

Důkaz nejbližšího následujícího jména

O účinnosti výše popsané změny návrhu svědčí skutečnost, že naše omezení určené původně pro KeyTrap je účinné i proti dalšímu čerstvě zveřejněnému útoku typu odepření služby (CVE-2023–50868).

Při něm útočník buď vybere, nebo vytvoří zónu podepsanou protokolem DNSSEC s parametry NSEC3 nakonfigurovanými v příkrém rozporu s doporučeným postupem RFC 9276, především s velkým množstvím **dodatečných iterací**. Poté proti této zóně provede útok pomocí dotazování na náhodné subdomény.

Bohužel se výše odkazované doporučení zatím **nedodržuje** u všech domén, resolvery obvykle musí akceptovat dodatečné NSEC3 iterace a spotřebovávají cykly procesoru na hašování SHA1.

Tyto dodatečné iterace haše SHA1 slouží jako další potenciální vektor útoku typu odepření služby. Příslušný standard, RFC 5155, oddíl 8.3, na toto riziko opět **neupozorňuje** a řada implementací se proti němu nechránila. Ironií osudu jsme tuto chybu objevili při testování nového omezení pro KeyTrap.

Novinkou u této zranitelnosti je uvědomění, že útočník může ovlivnit nejen použitou zónu, ale také počet opakování provedených algoritmem *Closest Encloser Proof* (důkaz nejbližšího následujícího jména). To útočníkovi umožňuje učinit útok zhruba **125× účinnějším**, než se dříve předpokládalo.

Naštěstí všechny verze serveru BIND vydané v roce 2023 již **omezily počet iterací** NSEC3 na maximálně 150 a hašovací algoritmus SHA1 je celkem efektivní, takže dopad na nejnovější verze BINDu (i před vydáním poslední opravy) je mnohem menší: k vyčerpání procesoru resolveru je třeba stovek dotazů za sekundu.

Smutné na tomto příběhu je, že kdyby všichni provozovatelé zón v DNS dodržovali **doporučované postupy**, implementace resolverů by mohly vynucovat přísnější omezení parametrů použitých pro NSEC3, čímž by se tento útok stal zcela neúčinným.

Dnes to ještě z praktických důvodů není reálné, ale my v ISC (Internet Systems Consortium) jsme odhodláni **zpřísnit limity** pro iterace NSEC3, jakmile to bude možné – vyzýváme proto provozovatele DNS: Přečtěte si prosím článek 3.1 v RFC 9276 a řiďte se jím!

Škálovatelnost DNS: dobrá, zlá, nebo šílená?

Není náhoda, že DNS ve vší obecnosti umožňuje nadměrné využívání prostředků: specifikace protokolu DNS záměrně nestanovují explicitní **omezení** mnoha parametrů. Mimo jiné to jsou:

- počet záznamů CNAME v řetězci – což vedlo k útoku DNS Unchained
- počet delegací při rekurzivním řešení dotazů – což vedlo k útoku NXNSAttack
- počet odpovědí na daný(é) zdroj(e) – což vedlo k zesilujícím útokům
- počet dotazů obecně – což vedlo k vynálezu útoků na náhodnou subdoménu
- počet validací – což vedlo k útoku KeyTrap
- počet iterací hašování NSEC3 – což vedlo ke vzniku CVE-2023–50868
- počet odpovědí v zónách s podporou ECS – což vedlo ke vzniku CVE-2023–5680
- počet… v podstatě čehokoliv

Možná si teď kladete otázku: jsou standardy protokolu DNS naprosto šílené?! Odpověď zní ne!

Kdyby standardy z roku 1987 zahrnovaly explicitní omezení všech těchto parametrů, nemohli bychom po celou tu dobu **škálovat** DNS, aniž bychom změnili protokol.

Představte si, že by byl pevně stanoven limit na počet kroků CNAME v řetězci: kdyby byl limit „maximálně dva CNAME“, nemohli bychom zkonstruovat dnešní sítě CDN (Content Delivery Networks). Pokud by byl stanoven limit na počet záznamů DNSKEY, například „maximálně dva DNSKEY“, nemohli bychom používat DNSSEC a zároveň mít pro jednu doménu více operátorů. Takto bychom mohli pokračovat. Absence limitů je na jedné straně nebezpečná, na druhé straně nám umožnila používat stejný protokol a škálovat ho beze změny už 37 let!

Neposlouchali jsme

Tvůrci protokolu DNS samozřejmě nebyli hloupí a tuto třídu problémů **předvídali**. Již v roce 1987 poskytli implementátorům několik obecných pokynů:

> Doporučené priority pro tvůrce resolveru jsou:
> 1. Omezit množství práce (odeslané pakety, paralelní procesy), aby se požadavek nemohl dostat do nekonečné smyčky nebo spustit řetězovou reakci požadavků či dotazů s jinými požadavky nebo dotazy, I KDYŽ NĚKDO ŠPATNĚ PŘIPRAVIL NĚKTERÁ DATA.

Čtete správně, již v roce 1987, kdy byla napsána původní specifikace DNS, bylo nejvyšší prioritou **omezení množství práce** prováděné implementací! Výzkumníci stále znovu a znovu nacházejí temná zákoutí, ve kterých nebyl tento obecný pokyn dodržen.

Zranitelnosti KeyTrap (CVE-2023–50387) a vyčerpání CPU při důkazu nejbližšího následujícího jména v NSEC3 (CVE-2023–50868) se tak připojily k řadě podobných zranitelností založených na **manipulaci** implementací DNS k nadměrné a zbytečné práci.

Pohled do zákulisí

Útoků tohoto typu bude přibývat, protože protokol DNS je notoricky známý svou složitostí. Naštěstí je v ekosystému DNS silná skupina implementátorů, kteří jsou (většinou) schopni spolu **otevřeně mluvit** a koordinovat odstraňování a zveřejňování těchto zranitelností.

Mnoho implementátorů DNS se zapojuje veřejně a sdílí zkušenosti s provozem a vývojem prostřednictvím DNS-OARC (DNS Operations, Analysis and Research Center). I my musíme poděkovat centru DNS-OARC za to, že nám všem poskytlo místo pro koordinaci a bezpečné kanály, které umožnily všem zúčastněným spolupracovat na zmírnění dopadu těchto dvou nedávných zranitelností.

Pokud se seriózně věnujete práci v oblasti DNS a dosud se neúčastníte DNS-OARC, je čas to zvážit. Připojte se k DNS-OARC a jejich diskusnímu serveru Mattermost a zúčastněte se jejich vynikajících seminářů!

Nezapomeňte na aktualizace

Výzkumný tým německého Národního výzkumného centra pro aplikovanou kybernetickou bezpečnost ATHENE zjistil v několika validátorech DNSSEC problém s implementací, který pramení z **nedostatku představivosti** vývojářů softwaru DNS, z absence výslovného upozornění ve standardech DNSSEC dle článku 5.3.3 v RFC 4035 a z nedodržování desítky let starých, velmi obecných rad.

Tyto útoky, které zneužívají složitost systému DNS, lze **naštěstí opravit**, aniž by se změnily základy protokolu. Změny provedené v serveru BIND a dalších DNS resolverech, které zmírňují tyto dvě zranitelnosti, zvýší jejich odolnost také proti dalším podobným útokům. Ekosystém DNS je ve zcela jiné pozici než například síť serverů pro uložení klíčů PGP SKS, kterou jeden útok založený na složitosti v podstatě učinil nepoužitelnou.

Protokol DNSSEC je i nadále bezpečný a poskytuje cennou ochranu před různými útoky na integritu systému DNS. Nejlepší reakcí na tuto zranitelnost je, aby operátoři **aktualizovali svůj software** na opravenou verzi.

Odkazy

CVE-2023–50387

- BIND 9 release announcement
- Unbound 1.19.1 release from NLnet Labs
- PowerDNS Recursor release announcement
- Knot Resolver release announcement
- Dnsmasq release announcement

ISC

- Reporting Security Vulnerabilities (to ISC)
- ISC Software Defect and Security Vulnerability Disclosure Policy
- ISC CVSS Scoring Guidelines
- BIND 9 Security Vulnerability Matrix

- History of BIND vulnerabilities by impact from CVE Details

Původně vyšlo na webu organizace ISC.

Vstoupit do diskuse

Autor článku

Petr Špaček

Pracuje jako analytik specializovaný na DNS. Podílí se na projektech BIND, DNS Shotgun a dnsperf. Dříve vyvíjel Knot DNS a Knot Resolver.

Témata:

BIND