Nový útok Denial-of-Service se zaměřuje na protokoly aplikační vrstvy

cispa.de/en/loop-dos

2024-03-19

Eva Micheliová

Loop DoS: Nový útok typu Denial-of-Service se zaměřuje na protokoly aplikační vrstvy

Nový útok DoS (Denial-of-Service) se zaměřuje na protokoly aplikační vrstvy, které využívají protokol UDP (User Datagram Protocol) pro end-to-end komunikaci. „Application-layer Loop DoS Attacks“ páruje servery těchto protokolů tak, že spolu komunikují neomezeně dlouho. Tato chyba zabezpečení se týká jak starších protokolů (např. QOTD, Chargen, Echo), tak současných (např. DNS, NTP a TFTP). Útok, který objevili výzkumníci z CISPA Helmholtz-Center for Information Security, ohrožuje odhadem 300 000 internetových hostitelů a jejich sítě.

mediální vydání

Nově objevený útok DoS smyčky se sám udržuje a zaměřuje se na zprávy aplikační vrstvy. Spáruje dvě síťové služby takovým způsobem, že si vzájemně odpovídají na zprávy donekonečna. Přitom vytvářejí velké objemy provozu, který má za následek odmítnutí služby pro zapojené systémy nebo sítě. Jakmile je vstříknuta spoušť a smyčka se dá do pohybu, ani útočníci nejsou schopni útok zastavit. Dříve známé smyčkové útoky se vyskytovaly na směrovací vrstvě jediné sítě a byly omezeny na konečný počet opakování smyčky.

Odhadem může být zneužito 300 000 internetových hostitelů

Výzkumníci CISPA Yepeng Pan a profesor Dr. Christian Rossow objevili útoky DoS smyčky aplikační vrstvy, které se pravděpodobně týkají celkem 300 000 internetových hostitelů. Pan a Rossow zatím potvrdili zranitelnost pro implementace TFTP, DNS a NTP a také pro šest starších protokolů Daytime, Time, Active Users, Echo, Chargen a QOTD. Tyto protokoly jsou široce používány k poskytování základních funkcí na internetu.

Zatímco NTP například umožňuje synchronizaci času mezi počítači, DNS přiřazuje názvy domén k jejich odpovídajícím IP adresám. TFTP umožňuje přenos souborů bez ověření uživatele.

Útoky mohou být spouštěny z jednoho hostitele schopného falšování

DoS útoky ve smyčce aplikační vrstvy se spoofují na IP spoofing a mohou být spuštěny z jednoho hostitele schopného spoofingu.„Útočníci by například mohli způsobit smyčku zahrnující dva vadné servery TFTP vložením jediné chybové zprávy s podvrženou IP adresou. Zranitelné servery by si pak nadále posílaly chybové zprávy TFTP, což by zatěžovalo oba servery a jakékoli síťové spojení mezi nimi," vysvětluje Rossow. Pan zdůrazňuje novost tohoto útočného vektoru: „Smyčky na aplikační úrovni, které jsme objevili, se liší od známých smyček na síťové vrstvě. Stávající kontroly doby životnosti paketů používané na síťové úrovni tedy nejsou schopny přerušit smyčky aplikační vrstvy.

Snadné zneužití

„Pokud víme, tento druh útoku nebyl v poli ještě proveden. Pro útočníky by však bylo snadné tuto zranitelnost zneužít, pokud by nebyla přijata žádná opatření ke zmírnění rizika," říká Rossow. V prosinci 2023 Rossow a Pan odhalili svůj objev dotčeným prodejcům a komunitě důvěryhodných operátorů. Dva výzkumní pracovníci CISPA koordinovali plán na zveřejnění doporučení specifického pro útok a společně s The Shadowserver Foundation zahájili oznamovací kampaň.

Počínaje 19. březnem 2024 bude poradenství specifické pro útok přístupné přes *https://cispa.saarland/group/rossow/Loop-DoS*