HTTP/2 Rapid Reset, la vulnerabilitat que permet llançar atacs DDoS amb un número de RPS rècord

2/11/23

ÍNDEX

1. Descripció de la Vulnerabilitat

1.1. Característiques del CVE-2023-44487

Recentment s'ha publicat la troballa d'una vulnerabilitat de dia zero que afecta el protocol HTTP/2, coneguda com a Ràpid Reset. Ha estat catalogada com a CVE-2023-44487, i se li ha atorgat una puntuació CVSS de 7,5.
Aquesta vulnerabilitat permet llançar atacs DDoS amb un nombre rècord de sol·licituds per segon (RPS, per les seves sigles en anglès) a causa de dos factors:

- Funcionalitat RST_Stream del protocol HTTP/2: la trama RST_Stream permet cancel·lar una sol·licitud enviada prèviament, i serveix per restablir connexions.
- Multiplexació: en l' àmbit de les telecomunicacions es coneix com a multiplexació la tècnica que permet combinar dos o més senyals i enviar-les mitjançant un únic mitjà de transmissió. És a dir, en aquest cas s'utilitza la tècnica de la multiplexació per combinar les sol·licituds utilitzades en un atac DDoS i enviar-les, simultàniament, a través d'una única connexió TCP.
- D'aquesta manera, els atacants van utilitzar la tècnica de la multiplexació per enviar de manera ràpida i successiva patrons de sol·licituds i cancel·lacions a connexions TCP úniques. Això comporta que botnets relativament no gaire grans tinguin la capacitat d'enviar números rècord de sol·licituds per segon i que els servidors siguin capaços de gestionar-les.

2. Vulnerabilitat HTTP/2 Rapid i atacs de DDoS

2.1 Nombre de sol·licituds record

Per entendre la veritable magnitud dels atacs DDoS que han explotat aquesta vulnerabilitat n'hi ha prou amb atendre les xifres que ha compartit el proveïdor Cloudflare: si al febrer anunciava haver aturat el major atac DDoS dirigit contra la seva infraestructura en el qual van patir fins a 71 milions de sol·licituds per segon (RPS), el CVE-2023-444 va possibilitar un atac en el qual es triplicaven les RPS, arribant a assolir les 201 milions.
Per la seva banda, Google Cloud també ha notificat un atac DDoS a la seva infraestructura que va assolir les 398 milions de RPS, mentre que AWS també s'ha vist afectat per un altre de 155 milions de RPS. Totes elles, xifres mai abans vistes

2.2. Possible relació entre la vulnerabilitat HTTP/2 Ràpid Reset i l'èxit de les campanyes d'atacs DDoS

Durant tot l'any 2023 s'ha experimentat un notable creixement de campanyes d'atacs DDoS orquestrades, principalment, per actors d'amenaça prorussos. De fet, a Espanya se n'han patit les conseqüències. La campanya d'atacs DDoS durant la jornada electoral va ser la que més impacte va tenir a causa de la seva repercussió mediàtica, ja que va aconseguir afectar llocs web tan rellevants com els del Ministeri de l'Interior, la Casa

Reial, o l'Institut Nacional d'Estadística, a més dels principals mitjans de comunicació digitals i entitats de telecomunicacions.
NoName(057) va estar després de la seva autoria i ha emprat aquestes campanyes a tall de resposta política contra aquells països que d'alguna manera s'ha posicionat a favor d'Ucraïna, com ha fet Espanya. D'alguna manera, molts investigadors i especialistes en ciberseguretat sempre han mostrat certa sorpresa per l'alta taxa d'èxit de les campanyes de NoName(057) perquè són un tipus d'atacs relativament fàcils de prevenir. Ara, a causa de conèixer la vulnerabilitat HTTP/2 Rapid Reset, es podria explicar aquest fet.
A això caldria unir que la vulnerabilitat Rapid Reset permet l'enviament d'un nombre de sol·licituds ingent amb una infraestructura de bots no gaire alta. A causa del seu projecte DDosia, una plataforma que en els seus començaments comptava amb uns 400 afiliats i que en poc més d'un any havia crescut un 2.400%, passant a sumar més de 10.000 usuaris. Actualment s'estima que pugui comptar amb entre 12.000 i 20.000 usuaris, tenint en compte que al seu canal de Telegram supera els 50.000 seguidors.

3. Recomanacions

3.1 Sobre mitigació

La vulnerabilitat HTTP/2 Rapid Request té una particularitat que dificulta la seva mitigació. En la majoria dels casos les vulnerabilitats afecten programaris que compten amb una firma darrere de proveir del parxís pertinent. Per exemple, si la bretxa de seguretat afectés Windows, la firma Microsoft seria l'encarregada d'oferir una actualització a tots els seus usuaris
En aquest cas la vulnerabilitat afecta una especificació d'un protocol web, per la qual cosa no hi ha una firma o entitat central que s'encarregui de la seva esmena, si no que són cadascun dels proveïdors web els responsables d'implementar les mesures pertinents. Cloudflare, Google, AWS, NGINX o Microsoft han notificat haver-lo parxís, però en cas de treballar amb qualsevol altre proveïdor seria imprescindible saber si també ho ha fet.
La bona notícia, tot i que no hi hagi una entitat central que treballi i coordini en la mitigació d'aquesta vulnerabilitat, és que el protocol HTTP/2 és de codi obert, per la qual cosa es pressuposa que en la majoria dels projectes en què s'apliqui s'haurà reutilitzat el codi dels grans proveïdors, per la qual cosa aplicar els pegats també serà una tasca relativament fàcil i àgil.

3.2 Enllaços d´interès

Més Informació:

- CISA: Comprender y responder a los ataques distribuidos de denegación de servicio
- Cloudflare: HTTP/2 Rapid Reset: deconstruyendo el ataque récord
- Google: Cómo funciona: el novedoso ataque DDoS HTTP/2 'Rapid Reset'

- AWS: CVE-2023-44487: ataque de reinicio rápido HTTP/2
- NGINX: Ataque de reinicio rápido HTTP/2 que afecta a los productos NGINX
- Microsoft: Respuesta de Microsoft a los ataques de denegación de servicio distribuido (DDoS) contra HTTP/2