Une vulnérabilité enrôle massivement pour amplifier les attaques DDoS

Plus de 100 000 appareils connectés en réseau pourraient être exploités pour lancer des attaques DDoS (Distributed Denial of Service). C'est la conséquence d'une vulnérabilité d'implémentation mDNS découverte par le chercheur en sécurité Chad Seaman et documentée auprès du CERT/Coordination Center dans cette alerte. Le mDNS (multicast Domain Name System) est un protocole qui permet aux appareils d'un réseau local de se reconnaître mutuellement à travers leur adresse IP sans passer par un serveur de noms. Un système utilisé tant par les PC que les disques réseau (NAS), imprimantes et tout autre appareil potentiellement connecté en IP, afin de simplifier la configuration du réseau.

Le protocole permet donc à une machine d'adresser une requête à une autre machine pour communiquer. La liste des différents éléments mDNS du réseau local étant stockée sur chacun des appareils. Normalement, le système doit vérifier que chaque requête adressée correspond bien à un appareil référencé dans le sous réseau. Dans le cas contraire, il doit ignorer la requête. Sauf que certains constructeurs n'ont visiblement pas suivi ces recommandations lors de l'implémentation du protocole dans leurs produits. Avec pour le risque d'autoriser la réponse à des requêtes issues de l'extérieur du réseau local, d'Internet notamment.

Réflecteurs de DDoS

Conséquence, une requête peut dévoiler des informations sur une machine locale (adresse MAC, numéro de série, nom d'hôte, configuration réseau…) et permettre à des attaquants d'établir une typologie du réseau de l'entreprise. Autre problème, *« alors que mDNS utilise l'UDP (protocole de transmission de données, NDLR), tous les hôtes qui répondent peuvent potentiellement être utilisés par des personnes malveillantes comme réflecteurs pour une campagne DDoS*, soulève Chad Seaman. *C'est aussi potentiellement amplifiable alors que les réponses tendent à être plus larges que les requêtes initiales. »* A travers ses propres tests, le chercheur a constaté des amplifications jusqu'à 975% de la taille de la requête même s'il estime à 130% la moyenne raisonnable de ses possibilités d'augmentation.

Rappelons que les attaques par déni de services distribués consistent à inonder un (ou plusieurs) serveurs cibles à l'aide d'un flux de requêtes IP continu pour le faire tomber ou ralentir sa performance (et éventuellement profiter de cette faiblesse pour pénétrer le réseau). Exploités en lançant des requêtes avec des adresses IP détournées (celle de la cible de l'attaque), ces appareils « relais » permettraient donc à des attaquants de se servir d'une infrastructure tierce pour cacher l'origine de leur attaque.

IBM, HP, Canon…

Parmi la centaine de millier de machines actuellement exploitables (qui répondent donc aux requêtes mDNS depuis Internet) repérées par le chercheur en sécurité, ce dernier note que la vulnérabilité touche aussi bien des imprimantes que des NAS comme des appareils sous Windows

et Linux (notamment à travers le logiciel Avahi mDNS). *« Certaines de ces machines étaient situés sur de grands réseaux tels que ceux d'entreprises et d'universités, et semblaient être mal sécurisées, quand elles l'étaient*, alerte Chad Seaman qui ajoute que *certains constructeurs ont déjà annoncé qu'ils ne corrigeraient pas la vulnérabilité sur des produits anciens, pourtant vulnérables. »* De son côté, le CERT fait état de Canon, HP, IBM ou encore Synology, comme fournisseurs de produits affectés.

Lire également

[La Chine suspectée d'une violente attaque DDoS sur GitHub]

[En 10 ans, les attaques DDoS se sont fortement amplifiées]

[Le site Defense.gouv se met à DDoS des Anonymous]

crédit photo © Duc Dao – shutterstock