Attaque par délégations DNS infinies « iDNS Attack »

ANSSI – contact@cert.ssi.gouv.fr

Le DNS est une base de données hiérarchique, utilisée pour publier des informations allant d'adresses IP à des politiques de sécurité. L'une des propriétés intrinsèques du DNS est la décentralisation des données. Le titulaire de noms de domaine peut, en effet, déléguer à un tiers son autorité sur un domaine enfant, appelé « sous-domaine ».

L'ANSSI a découvert une vulnérabilité affectant la manière dont plusieurs implémentations de serveurs DNS récursifs suivent les délégations. Cette vulnérabilité a pour origine des contrôles insuffisants ou inexistants sur le nombre de délégations qu'un résolveur accepte de suivre pour résoudre un nom de domaine.

L'attaque par délégations DNS infinies permet d'engager un résolveur DNS à suivre une suite « infinie » de délégations. Il peut y être incité à l'aide d'une unique requête émise par un client légitime de ce serveur DNS récursif. De plus amples détails sont fournis dans l'annexe technique de ce document. Cette attaque permet de mener deux types de dénis de service. Leur nature exacte varie suivant l'implémentation exploitée.

D'une part, certains résolveurs suivent toutes les délégations simultanément, générant ainsi un pic de trafic vers une destination au choix de l'attaquant. Il peut en résulter alors un déni de service distribué, avec une forte amplification du nombre de paquets. Il convient de noter que ces paquets sont indistinguables du trafic légitime émis par les serveurs DNS récursifs exploités par l'attaquant. La dépollution de trafic par la victime de l'attaque peut donc s'avérer difficile. Par ailleurs, ce type de déni de service se distingue par sa capacité à effectuer un déni de service distribué sans avoir recours à l'usurpation d'adresses IP.

D'autre part, cette attaque peut être employée pour effectuer un déni de service sur le serveur DNS récursif d'un opérateur. Dans ce cas de figure, il convient de noter que cette attaque nécessite une unique requête par un client légitime, puis l'échange de plusieurs centaines de milliers de paquets entre des serveurs DNS faisant autorité sur des zones sous contrôle de l'attaquant et le serveur DNS récursif attaqué. L'impact varie alors de l'interruption totale de service, à la consommation excessive de ressources système et la forte réduction de la qualité du service, avec des temps de réponse significativement plus longs.

Toutes les versions de BIND (CVE-2014-8500), Unbound (CVE-2014-8602) et PowerDNS (CVE-2014-8601) sont vulnérables à cette attaque, avec des degrés de sévérité variant d'un logiciel à l'autre. La vulnérabilité a été confirmée par des expériences en laboratoire et par les fournisseurs de ces logiciels. Dans le cas de BIND, l'ANSSI a, de plus, identifié un défaut dans le cloisonnement entre le rôle de serveur récursif et de serveur faisant autorité. Ce problème permet également d'attaquer un serveur faisant autorité, même configuré pour complètement désactiver la récursion, s'il héberge des zones pouvant contenir des données contrôlées par un attaquant.

Les serveurs d'OpenDNS, de Google Public DNS et de Microsoft DNS sur Windows Server 2012 ne sont pas vulnérables.

L'ANSSI recommande à tous les fournisseurs de logiciels de serveurs DNS récursifs d'implémenter une limite sur la quantité ressources système allouées à la résolution d'un nom de domaine, et à toutes les requêtes pouvant en résulter. OpenDNS, contacté pour obtenir un retour opérationnel sur cette recommandation, a confirmé avoir déjà déployé ce type de contremesures sans avoir subi de dégradation sur la qualité de leur service en mode nominal.

L'ANSSI recommande à tous les opérateurs de mettre à jour dès que possible leurs serveurs DNS. Les versions bénéficiant des correctifs de sécurité sont BIND 9.9.6-P1, BIND 9.10.1-P1, Unbound 1.5.1, et PowerDNS Recursor 3.6.2.

L'ANSSI recommande également aux opérateurs d'évaluer si des équipements intermédiaires pourraient être affectés négativement par la forte augmentation de trafic pouvant être induite par l'exploitation de leurs serveurs DNS lors de la mise en œuvre de cette attaque, ou d'une variante.