Résolveur DNS

Vous avez peut-être récemment reçu un courrier et/ou un e-mail de la part de Sunrise vous informant qu'un appareil de votre réseau présente une vulnérabilité de résolveur DNS ouvert. Si vous avez reçu cette communication de notre part, veuillez lire les conseils donnés sur cette page destinés à vous aider à résoudre le problème.

Remarque: cet article a pour but de vous conseiller. Sunrise n'est toutefois pas responsable des problèmes rencontrés lors de la résolution de problème et n'est pas en mesure de fournir une assistance technique pour de tels cas.

Aperçu

Le Domain Name System (DNS) est un système utilisé par les ordinateurs pour convertir des noms de domaine en adresse IP sur Internet. Un serveur DNS est un système qui accepte les demandes d'autres systèmes informatiques pour convertir des domaines en adresses IP.

Un résolveur DNS récursif ouvert est un serveur DNS qui a été ouvert aux demandes DNS depuis n'importe quel système informatique sur Internet. Si ces serveurs sont mal configurés, ils peuvent être utilisés pour participer indépendamment de votre volonté à des activités malveillantes.

Que s'est-il passé?

Nous travaillons avec un certain nombre d'organisations à but non lucratif dans tous les secteurs de la sécurité qui collectent des informations sur des appareils qui semblent être compromis ou mal configurés sur Internet. Votre appareil est donc défectueux ou mal configuré et accessible publiquement sur Internet, et donc la numérisation effectuée par ces organisations ne se trouve pas dans votre réseau privé.

Nous suspectons qu'un appareil connecté à votre réseau domestique présente une vulnérabilité de résolveur DNS ouvert.

Pour plus d'informations sur ces rapports, rendez-vous sur dnsscan.shadowserver.org

Si les paramètres sont laissés ouverts, ils peuvent être utilisés pour participer indépendamment de votre volonté à des activités malveillantes, comme une attaque DDoS (attaque par déni de service).

Il est donc important de suivre les conseils de cet article.

Remarque: cet article a pour but de vous conseiller. Sunrise n'est toutefois pas responsable des problèmes rencontrés lors de la résolution de problème et n'est pas en mesure de fournir une assistance technique pour de tels cas.

Fermeture du port vulnérable

Le moyen le plus simple de gérer un résolveur DNS ouvert est de configurer votre pare-feu pour bloquer le port 53 afin d'empêcher les demandes DNS provenant de l'extérieur de votre réseau domestique.

Si vous avez besoin d'une résolution DNS capable de répondre aux demandes extérieures provenant d'Internet, veuillez vous assurer que votre serveur est configuré pour n'accepter que le trafic résultant d'adresses IP.

Pour fermer le port vulnérable:

- Accédez à la page de configuration de votre routeur
- Connectez-vous avec votre nom d'utilisateur et votre mot de passe affichés par défaut sur le routeur lui-même
- Sélectionnez l'option Redirection de port (Port Forwarding)
- Supprimez toutes les règles qui permettent l'ouverture du port 53

- Sélectionnez l'option Déclenchement du port (Port Triggering)
- Supprimez toutes les règles qui permettent l'ouverture du port 53

Questions au sujet d'Internet

Sunrise est co-fondateur et membre de iBarry.ch, une organisation à but non lucratif qui travaille avec des experts en sécurité informatique afin de vous fournir toutes les informations dont vous avez besoin pour que vos enfants et vous surfiez en ligne en toute sécurité.

Pour plus d'informations sur iBarry, rendez-vous sur https://www.ibarry.ch/fr/