Portmapper

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

Aperçu

Il y a un défaut de conception dans le service Portmapper actuellement utilisé sur un appareil de votre réseau domestique. Portmapper, également appelé RPC Bind ou RPC Portmap, est un service utilisé par des systèmes informatiques pour assister les tâches réseau.

Ce défaut peut permettre à un tiers d'accéder à distance à des accès non autorisés et d'effectuer des attaques de type déni de service (DDoS) contre des machines cibles. Un pirate informatique à distance peut exploiter cette erreur en envoyant une demande spécialement adaptée à un serveur Portmapper concerné.

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 Portmapper.

Pour plus d'informations sur ces rapports, rendez-vous sur portmapperscan.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.

Comment résoudre le problème?

Le moyen le plus simple de gérer une vulnérabilité de Portmapper est de configurer votre pare-feu pour bloquer le port UDP 111.

Veuillez noter que le blocage de ce port interrompt uniquement le trafic sortant ou entrant dans votre réseau domestique. Les services de votre logement qui utilisent ce port devraient continuer à fonctionner normalement.

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 laisseront le port 111 ouvert
- Sélectionnez l'option Déclenchement du port (Port Triggering)
- Supprimez toutes les règles qui laisseront le port 111 ouvert

Assurez-vous que tous les appareils de votre réseau soient protégés par un pare-feu. Il est important de vérifier que tous vos appareils sont couverts par un pare-feu.

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/

Version: 12.2021