Protocole SNMP

Vous avez peut-être récemment reçu un courrier et/ou un e-mail de la part de Sunrise vous expliquant qu'un appareil de votre réseau présente une brèche du protocole SNMP (Simple Network Management Protocol). Si vous avez reçu cette communication de notre part, veuillez suivre les conseils donnés sur cette page afin de résoudre le problème.

Aperçu

Le protocole SNMP (Simple Network Management Protocol) est une méthode permettant de gérer ou d'accéder à distance à un appareil depuis et sur un réseau informatique. Une vulnérabilité SNMP est un problème de sécurité qui permet à un tiers d'utiliser ce protocole pour obtenir un accès non autorisé à votre réseau/aux appareils à des fins malveillantes si le protocole est configuré de manière incorrecte.

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 brèche SNMP.

Pour plus d'informations sur ces rapports, rendez-vous sur snmpscan.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 les menaces et brèches SNMP est de configurer votre pare-feu pour bloquer les ports UDP 161 et 162.

Veuillez noter que le blocage de ces ports interrompt uniquement le trafic sortant ou entrant dans votre réseau domestique. Les services de votre domicile utilisant les ports 161 et 162 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 permettent l'ouverture des ports 161 et 162
- Sélectionnez l'option Déclenchement du port (Port Triggering)
- Supprimez toutes les règles qui permettent l'ouverture des ports 161 et 162

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