EBDS
WIRELESS & ANTENNAS

Bulletin technique

Date d'émission : 16/04/2018

Date d'application : Immédiat

Type : Menace

Marque : Sierra Wireless

Technologie : 2G, 3G, 4G

Produit(s) concerné(s) :

- LS300 avec firmware version 4.4.1 ou antécédente
- GX450, ES450, RV50, RV50X, MP70 avec firmware version 4.8.1 ou antécédente

Intitulé : Menace IoTroop/Reaper sur les routeurs ayant une version ancienne du firmware

Contenu

Sierra Wireless a détecté une menace sur les routeurs de la gamme Airlink fonctionnant sur une ancienne version du firmware, qui utilisent le mot de passe usine et qui sont atteignables depuis les réseaux internet publics (IP publique).

Si vous utilisez un VPN ou faites uniquement de l'accès sortant, vous ne serez pas impacté.

1. Produits concernés

Modèle	Version firmware touchée
LS300, GX400, GX/ES440	ALEOS 4.4.1 ou antécédente
GX/ES450, RV50, RV50X, MP70, MP70E	ALEOS 4.8.1 ou antécédente

Veuillez prendre en compte le fait que cela concerne également les routeurs qui ont été mis à jour par la suite vers les versions 4.9.0, 4.9.1 ou 4.4.5.

2. Description du problème technique

Sierra Wireless a détecté une intrusion IoTroop/Reaper sur certains de ses routeurs et prend cette menace très au sérieux. Sierra Wireless travaille activement avec les clients qui ont été touchés par ce problème pour y remédier. Tout est mis en place pour que cette menace soit écartée le plus rapidement possible.

Le logiciel malveillant concerné est connu pour impacter les routeurs de la manière suivante :

a) Pendant l'installation de cette menace, le mot de passe de l'utilisateur est volé et envoyé directement à un serveur de contrôle. Le routeur peut alors être réinfecté par la suite si le mot de passe n'est pas modifié.
b) Ce logiciel malveillant pourra alors fréquemment envoyer des instructions au serveur de contrôle et potentiellement participer à une attaque de Déni de Service (DDoS). Cela augmentera alors considérablement le temps de chargement de vos données et les rendra indisponibles.

Il est conseillé à tous nos clients de suivre immédiatement des actions que nous vous recommandons ci-dessous. Cette manipulation permettra de protéger vos routeurs de cette menace et de la faire disparaitre de vos routeurs si celle-ci est déjà présente sur l'équipement.

3. Recommandations

Sierra Wireless recommande fortement que les clients qui utilisent des routeurs atteignables depuis les réseaux internet publics **opèrent cette manipulation immédiatement**.

1) **MISE A JOUR**.
Pour vous assurer que la menace n'est plus présente sur votre routeur, veuillez mettre à jour le firmware avec la version correspondante dès que celle-ci sera disponible

Modèle	Version firmware à télécharger
LS300, GX400, GX/ES440	ALEOS 4.4.6 ou suivante
GX/ES450, RV50, RV50X, MP70, MP70E	ALEOS 4.9.2 ou suivante

2) **CHANGEMENT DU MOT DE PASSE**.
Après avoir effectué la mise à jour, veuillez immédiatement changer le mot de passe utilisateur sur tous les routeurs pour plus de sécurité, même si les routeurs possédaient déjà un mot de passe différent du mot de passe usine.

a. Dans ACEmanager, cliquez sur *Admin* > *Change password*
b. Si vous utilisez AirLink Management Service (ALMS), suivez les instructions sur cette page :

https://doc.airvantage.net/alms/reference/monitor/howtos/remotelyChangeACEManagerPassword/

La configuration des changements et la mise à jour du firmware peut être fait individuellement sur chaque routeur en utilisant ACEmanager ou sur plusieurs routeurs en même temps en utilisant AirLink Management Service (ALMS). ALMS est gratuit pour les clients ayant jusqu'à 15 routeurs.

3) **DESACTIVER L'ACCES DISTANT OU FILTRER LES ADRESSES IP**.

- Désactiver l'accès distant pour éviter les intrusions d'équipements et de personnes non autorisés. L'accès distant (Remote Access) est désactivé par défaut et il est important qu'il le reste. Pour cela : Dans AceManager > Remote Access >Cliquez sur « Disable »

  OU

- Filtrer les adresses IP pour réduire l'accès aux personnes autorisées. Vous devez réaliser une redirection de port ou une DMZ. Pour cela : Dans ACEManager > Security > Trusted IP

Plus d'informations

Pour plus d'informations ou un support technique, n'hésitez pas à nous contacter au

09 72 36 76 46 ou par email à **info@ebds.eu**

EBDS décline toute responsabilité quant à l'utilisation des informations contenues dans ce document. Celles-ci sont uniquement fournies à titre informatif et n'entraînent aucune obligation légale.

- Source Sierra Wireless :

https://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---reaper/

- Bulletin technique de Sierra Wireless :

https://source.sierrawireless.com/~/media/support_downloads/airlink/docs/technical%20bulletin/swi-psa-2018-002%20technical%20bulletin%20-%20reaper%20-%2029mar2018.ashx?la=en