Pièce jointe (contenu sur notre site Web)

Date de sortie : 16 octobre 2024
Dernière mise à jour : 18 octobre 2024

Notice

Pour les clients utilisant le système IXG du système résidentiel IP

Nous vous remercions pour votre soutien continu concernant nos produits.

Nous vous informons que le Système IX du réseau IP Audio-Video Intercom, que nous vendons depuis mai 2020, s'est révélé être vulnérable à une attaque utilisant une technologie spécialisée qui pourrait entraîner la fuite des données stockées dans le produit cible ou la perte d'une partie des fonctions du produit.

■ Produits cibles

・Poste du locataire: IXG-2C7, IXG-2C7-L

・Platine d’entrée: IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K

・Poste du gardien: IXG-MK

・Adaptateur passerelle: IXGW-GW, IXGW-TGW

・Adapt. contr. ascenseur: IXGW-LC

・Outil d’assistance IXG

■ Version cible

1. CVE-2024-31408、CVE-2024-39290

・ IXG-2C7, IXG-2C7-L, IXGW-GW, IXGW-TGW: toutes les versions antérieures à Ver. 3.01

・ IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K, IXG-MK, IXGW-LC: toutes les versions antérieures à Ver. 3.00

2. CVE-2024-47142

・ IXG-2C7, IXG-2C7-L：toutes les versions antérieures à Ver. 2.03

3. CVE-2024-45837

・ IXG-2C7, IXG-2C7-L, IXGW-GW, IXGW-TGW: toutes les versions antérieures à Ver.3.01

・ IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K, IXG-MK, IXGW-LC: toutes les versions antérieures à Ver. 3.00

・ Outil d’assistance IXG: toutes les versions antérieures à Ver. 5.0.2.0

* Veuillez vérifier « Liste des produits cibles » pour les images et les versions de produit avant et après les contre-mesures.

■ Description de la vulnérabilité

Il est possible qu'un tiers ayant accès à ce produit via un réseau puisse lire, modifier, supprimer et/ou manipuler les données. Du fait que cette attaque nécessite une technologie très spécialisée, il n'y a pas eu de rapports signalant des dommages causés par cette attaque depuis le lancement de ce produit.

■ Contre-mesures

Si vous utilisez une version ciblée, veuillez télécharger le micrologiciel avec la contre-mesure depuis Logiciel et documents et mettez à jour le produit ciblé.

■ Contact pour toute demande de renseignements

Si vous êtes un client utilisant un produit ciblé et si vous avez des questions à ce sujet, n'hésitez pas à nous contacter. Nous vous contacterons à l'adresse e-mail que vous avez fournie.

▸Nous contacter
https://www.aiphone.net/support/contact/

Les informations personnelles fournies par le client ne seront pas utilisées à d'autres fins que pour ce sujet. Veuillez vérifier https://www.aiphone.net/privacy/ pour notre politique de confidentialité.

■ Informations de référence
JVN# 41397971/CVE-2024-31408/CVE-2024-39290/CVE-2024-45837/CVE-2024-47142

16 Octobre 2024
AIPHONE CO., LTD.

○ Liste des produits ciblés

Nom du produit	N° de modèle	Image du produit	CVE-2024-31408、CVE-2024-39290		CVE-2024-47142		CVE-2024-45837	
			Version avant les contre-mesures	Version après les contre-mesures	Version avant les contre-mesures	Version après les contre-mesures	Version avant les contre-mesures	Version après les contre-mesures
Poste du locataire	IXG-2C7	 IXG-2C7	Ver3.01	Ver4.00	Ver2.03	Ver2.04	Ver3.01	Ver4.00
	IXG-2C7-L	 IXG-2C7-L	Ver3.01	Ver4.00	Ver2.03	Ver2.04	Ver3.01	Ver4.00
Platine d'entrée	IXG-DM7	 IXG-DM7	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
	IXG-DM7-HID	 IXG-DM7-HID	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
	IXG-DM7-HIDA	 IXG-DM7-HIDA	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
	IXG-DM7-10K	 IXG-DM7	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Poste du gardien	IXG-MK	 IXG-MK	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Adaptateur passerelle	IXGW-GW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
	IXGW-TGW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
Adapt. contr. ascenseur	IXGW-LC	 IXGW-LC	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Outil d'assistance IXG	-	-	-	-	-	-	Ver5.0.2.0	Ver6.0.0.0