Documento adjunto (Contenido de nuestro sitio web)

Fecha de lanzamiento: 16 de octubre de 2024
Última actualización: 18 de octubre de 2024

Aviso

Para los clientes que usen IP-based Residential System IXG System

Gracias por su continuo apoyo adquiriendo nuestros productos.

Le informamos de que el IP-based Residential System IXG System, que hemos estado vendiendo desde mayo del 2020, ha sido determinado como vulnerable a ataques usando una tecnología especializada que podría resultar en la filtración de los datos almacenados en el producto objetivo o la pérdida de parte de las funciones del producto.

■ Productos objetivo

・Arrendatario estación: IXG-2C7, IXG-2C7-L

・Estación de entrada: IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K

・Estación de conserje: IXG-MK

・Adapt. puerta de enlace: IXGW-GW, IXGW-TGW

・Adapt. control ascen.: IXGW-LC

・Herramienta de soporte de IXG

■ Versiones

1. CVE-2024-31408、CVE-2024-39290

・ IXG-2C7, IXG-2C7-L, IXGW-GW, IXGW-TGW: Todas las versiones anteriores a Ver. 3.01

・ IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K, IXG-MK, IXGW-LC: Todas las versiones anteriores a Ver. 3.00

2. CVE-2024-47142

・ IXG-2C7, IXG-2C7-L：Todas las versiones anteriores a Ver. 2.03

3. CVE-2024-45837

・ IXG-2C7, IXG-2C7-L, IXGW-GW, IXGW-TGW: Todas las versiones anteriores a Ver. 3.01

・ IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K, IXG-MK, IXGW-LC: Todas las versiones anteriores a Ver. 3.00

・ Herramienta de soporte de IXG: Todas las versiones anteriores a Ver. 5.0.2.0

* Consulte “Lista de productos objetivo” para ver las imágenes y versiones del producto antes y después de las contramedidas.

■ Descripción de la vulnerabilidad

Existe la posibilidad de que un tercero que tenga acceso a este producto a través de una red pueda leer, alterar, eliminar y/o manipular los datos. Debido a que este ataque requiere una tecnología altamente especializada, no se han reportado daños causados por este ataque desde el lanzamiento de este producto.

■ Contramedidas

Si está utilizando una versión objetivo, descargue el firmware con la contramedida desde Software y Documentos y actualice el producto de destino.

■ Contacto para consultas

Si usted es un cliente que utiliza un producto objetivo y tiene cualquier pregunta relacionada con este tema, no dude en ponerse en contacto con nosotros. Nos pondremos en contacto con usted a través de la dirección de correo electrónico proporcionada.

▸Contacto
https://www.aiphone.net/support/contact/

La información personal proporcionada por el cliente no se utilizará para ningún otro propósito que no sea este asunto. Consulte nuestra política de privacidad en https://www.aiphone.net/privacy/.

■ Información de referencia
JVN# 41397971/CVE-2024-31408/CVE-2024-39290/CVE-2024-45837/CVE-2024-47142

16 de Octubre de 2024
AIPHONE CO., LTD.

○ Lista de productos objetivo

Nombre del producto	N.º de modelo	Imagen del producto	CVE-2024-31408、CVE-2024-39290		CVE-2024-47142		CVE-2024-45837	
			Versión anterior a las contramedidas	Versión posterior a las contramedidas	Versión anterior a las contramedidas	Versión posterior a las contramedidas	Versión anterior a las contramedidas	Versión posterior a las contramedidas
Arrendatario estación	IXG-2C7		Ver3.01	Ver4.00	Ver2.03	Ver2.04	Ver3.01	Ver4.00
	IXG-2C7-L		Ver3.01	Ver4.00	Ver2.03	Ver2.04	Ver3.01	Ver4.00
Estación de entrada	IXG-DM7		Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
	IXG-DM7-HID		Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
	IXG-DM7-HIDA		Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
	IXG-DM7-10K		Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Estación de conserje	IXG-MK		Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Adapt. puerta de enlace	IXGW-GW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
	IXGW-TGW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
Adapt. control ascen.	IXGW-LC		Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Herramienta de soporte de IXG	-	-	-	-	-	-	Ver5.0.2.0	Ver6.0.0.0