

Notice

For customers using IP-based Residential System IXG System

Thank you for your continued support of our products.

We are informing you that IP-based Residential System IXG System, which we have been selling since May 2020, has been found to be vulnerable to an attack using specialized technology that could result in the leakage of data stored in the target product or the loss of part of the product's functions.

■ Target Products

- Tenant Station: IXG-2C7, IXG-2C7-L
- Entrance Station: IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K
- Guard Station: IXG-MK
- Gateway Adaptor: IXGW-GW, IXGW-TGW
- Lift Control Adaptor: IXGW-LC
- IXG Support Tool

■ Target Versions

1. CVE-2024-31408, CVE-2024-39290

- IXG-2C7, IXG-2C7-L, IXGW-GW, IXGW-TGW: All versions prior to Ver. 3.01
- IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K, IXG-MK, IXGW-LC: All versions prior

to Ver. 3.00

2. CVE-2024-47142

- IXG-2C7, IXG-2C7-L: All versions prior to Ver. 2.03

3. CVE-2024-45837

- IXG-2C7, IXG-2C7-L, IXGW-GW, IXGW-TGW: All versions prior to Ver. 3.01
- IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K, IXG-MK, IXGW-LC: All versions prior

to Ver. 3.00

- IXG Support Tool: All versions prior to Ver. 5.0.2.0

* Please check "List of Target Products" for product images and versions before and after countermeasures.

■ Description of Vulnerability

There is a possibility that a third party who has access to this product via a network may read, alter, delete, and/or manipulate the data. Because this attack requires highly specialized technology, there have been no reports of damage caused by this attack since the launch of this product.

■ Countermeasures

If you are using a target version, please download the firmware with the countermeasure from [Software and Documents](#) and update the target product.

■ Contact for inquiries

If you are a customer using a target product and have any questions regarding this matter, please feel free to contact us. We will contact you at the e-mail address you provided.

▶Contact us

<https://www.aiphone.net/support/contact/>











Personal information provided by the customer will not be used for any purpose other than this matter. Please check <https://www.aiphone.net/privacy/> for our privacy policy.

■ Reference information

JVN# 41397971/CVE-2024-31408/CVE-2024-39290/CVE-2024-45837/CVE-2024-47142

October 16, 2024
AIPHONE CO., LTD.

○ List of Target Products

Product Name	Model No.	Product Image	CVE-2024-31408、CVE-2024-39290		CVE-2024-47142		CVE-2024-45837	
			Version before Countermeasures	Version after Countermeasures	Version before Countermeasures	Version after Countermeasures	Version before Countermeasures	Version after Countermeasures
Tenant Station	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
Entrance Station	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
Guard Station	IXG-MK	 IXG-MK	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Gateway Adaptor	IXGW-GW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
	IXGW-TGW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
Lift Control Adaptor	IXGW-LC	 IXGW-LC	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
IXG Support Tool	-	-	-	-	-	-	Ver5.0.2.0	Ver6.0.0.0