

Kennisgeving

Voor klanten die het IP-gebaseerd residentieel systeem IXG-systeem gebruiken

Bedankt voor uw voortdurende steun aan onze producten.

Wij informeren u dat het IP-gebaseerd residentieel systeem IXG-systeem, dat wij sinds Mei 2013 verkopen, kwetsbaar is gebleken voor een aanval door middel van gespecialiseerde technologie die kan leiden tot het lekken van gegevens die opgeslagen zijn in het doelproduct of het verlies van een deel van de functies van het product.

■ Doelproducten

- Huurdersstation: IXG-2C7, IXG-2C7-L
- Ingangsstation: IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K
- Conciërgepost: IXG-MK
- Gatewayadapter: IXGW-GW, IXGW-TGW
- Liftbesturingsadapter: IXGW-LC
- IXG Support Tool

■ Doelversie

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

* Controleer "Lijst met doelproducten" voor productafbeeldingen en -versies voor en na tegenmaatregelen.

■ Beschrijving van kwetsbaarheid

De mogelijkheid bestaat dat een derde die toegang heeft tot dit product via een netwerk de gegevens kan lezen, wijzigen, verwijderen en/of manipuleren. Aangezien deze aanval een zeer gespecialiseerde technologie vereist, zijn er geen meldingen van schade veroorzaakt door deze aanval sinds de lancering van dit product.

■ Tegenmaatregelen

Als u een doelversie gebruikt, download dan de firmware met de tegenmaatregel van [Software en documenten](#) en werk het doelproduct bij.

■ Neem contact op voor vragen

Als u een klant bent die een doelproduct gebruikt en vragen heeft over deze kwestie, neem dan gerust contact met ons op. Wij zullen contact met u opnemen via het e-mailadres dat u heeft opgegeven.

►Neem contact met ons op

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

Persoonlijke informatie die door de klant wordt verstrekt, zal niet worden gebruikt voor enig ander doel dan dit. Raadpleeg <https://www.aiphone.net/privacy/> voor ons privacybeleid.

■ Referentie-informatie

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

16 Oktober 2024
AIPHONE CO., LTD.

O Lijst met doelproducten

Productnaam	Modelnr.	Productafbeelding	CVE-2024-31408	CVE-2024-39290	CVE-2024-47142		CVE-2024-45837	
			Versie vóór tegenmaatregelen	Versie na tegenmaatregelen	Versie vóór tegenmaatregelen	Versie na tegenmaatregelen	Versie vóór tegenmaatregelen	Versie na tegenmaatregelen
Huurdersstation	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
Ingangsstation	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
Conciërgepost	IXG-MK	 IXG-MK	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Gatewayadapter	IXGW-GW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
	IXGW-TGW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
Liftbesturingsadapter	IXGW-LC	 IXGW-LC	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
IXG Support Tool	-	-	-	-	-	-	Ver5.0.2.0	Ver6.0.0.0