Anhang (Inhalt auf unserer Website)

Erscheinungsdatum: 16. Oktober 2024
Letzte Aktualisierung: 18. Oktober 2024

Hinweis

Für Kunden, die das IP-basierte Wohngebäudesystem IXG System verwenden

Vielen Dank für Ihre andauernde Unterstützung unserer Produkte.

Wir informieren Sie darüber, dass das IP-basierte Wohngebäudesystem IXG System, das wir seit dem Mai 2020 verkaufen, sich als anfällig für einen Angriff mit spezialisierter Technologie erwiesen hat, der dazu führen könnte, dass auf einem betroffenen Produkt gespeicherte Daten abgegriffen werden oder ein Teil der Produktfunktionen verloren gehen.

■ Betroffene Produkte

・Mieter-Station: IXG-2C7, IXG-2C7-L

・Eingangsstation: IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K

・Pförtner-Station: IXG-MK

・Gateway-Adapter: IXGW-GW, IXGW-TGW

・Aufzugssteuerungsadap : IXGW-LC

・IXG Support Tool

■ Betroffene Versionen

1. CVE-2024-31408、CVE-2024-39290

・ IXG-2C7, IXG-2C7-L, IXGW-GW, IXGW-TGW: Alle Versionen vor Ver. 3.01

・ IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K, IXG-MK, IXGW-LC: Alle Versionen vor Ver. 3.00

2. CVE-2024-47142

・ IXG-2C7, IXG-2C7-L：Alle Versionen vor Ver. 2.03

3. CVE-2024-45837

・ IXG-2C7, IXG-2C7-L, IXGW-GW, IXGW-TGW: Alle Versionen vor Ver. 3.01

・ IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K, IXG-MK, IXGW-LC: Alle Versionen vor Ver. 3.00

・ IXG Support Tool: Alle Versionen vor Ver. 5.0.2.0

* Produktbilder und Informationen zur Version vor und nach Gegenmaßnahmen finden Sie in der „Liste der betroffenen Produkte“.

■ Beschreibung der Schwachstellen

Es besteht die Möglichkeit, dass Dritte, die über ein Netzwerk Zugriff auf dieses Produkt haben, die Daten lesen, ändern, löschen und/oder bearbeiten können. Da dieser Angriff eine hoch spezialisierte Technologie erfordert, gibt es seit der Einführung dieses Produkts keine Berichte über Schäden, die durch einen solchen Angriff verursacht wurden.

■ Gegenmaßnahmen

Wenn Sie eine betroffene Version verwenden, laden Sie die Firmware mit der Gegenmaßnahme von Software und Dokumente herunter und aktualisieren Sie das betroffene Produkt.

■ Kontakt für Anfragen

Wenn Sie ein Kunde mit einem betroffenen Produkt sind und Fragen zu dieser Angelegenheit haben, wenden Sie sich bitte an uns. Wir werden unter der von Ihnen angegebenen E-Mail-Adresse auf Sie zukommen.

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

Vom Kunden bereitgestellte persönliche Daten werden ausschließlich in dieser Angelegenheit genutzt. Informationen zu unserer Datenschutzrichtlinie finden Sie unter https://www.aiphone.net/privacy/.

■ Referenzinformationen

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

16. Oktober 2024
AIPHONE CO., LTD.

○ Liste der betroffenen Produkte

Produktname	Modell-Nr.	Produktbild	CVE-2024-31408、CVE-2024-39290		CVE-2024-47142		CVE-2024-45837	
			Version vor den Gegenmaßnahmen	Version nach Gegenmaßnahmen	Version vor den Gegenmaßnahmen	Version nach Gegenmaßnahmen	Version vor den Gegenmaßnahmen	Version nach Gegenmaßnahmen
Mieter-Station	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
Eingangsstation	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
Pförtner-Station	IXG-MK		Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Gateway-Adapter	IXGW-GW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
	IXGW-TGW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
Aufzugssteuerungsadap.	IXGW-LC		Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
IXG Support Tool	-	-	-	-	-	-	Ver5.0.2.0	Ver6.0.0.0