

Bildirim

IP Tabanlı Konut Sistemi IXG Sisteminin kullanan müşteriler için

Ürünlerimize verdiğiniz sürekli destek için teşekkür ederiz.

Mayıs 2020'ten beri sattığımız IP Tabanlı Konut Sistemi IXG Sisteminin, hedef üründe depolanan verilerin sızmasına veya ürünün fonksiyonlarının bir kısmının kaybolmasına neden olabilecek özel bir teknoloji kullanılarak yapılabilecek bir saldırıya karşı savunmasız olduğu tespit edilmiştir.

■ Hedef Ürünler

- Kiracı İstasyonu: IXG-2C7, IXG-2C7-L
- Giriş İstasyonu: IXG-DM7, IXG-DM7-HID, IXG-DM7-HIDA, IXG-DM7-10K
- Koruma İstasyonu: IXG-MK
- Ağ Geçidi Adaptörü: IXGW-GW, IXGW-TGW
- Asansör Kont. Adaptörü: IXGW-LC
- IXG Destek Aracı

■ Hedef Versiyonları

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 Destek Aracı: All versions prior to Ver. 5.0.2.0

* Lütfen önlemler öncesinde ve sonrasında ürün görüntüleri ve sürümleri için “Hedef Ürünler Listesi” dosyasını kontrol edin.

■ Zaafiyetin Tanımı

Bir ağ üzerinden bu ürüne erişimi olan üçüncü bir tarafın verileri okuması, değiştirmesi, silmesi ve/veya manipüle etmesi mümkündür. Bu saldırı oldukça özelleştirilmiş teknolojiler gerektirdiğinden, bu ürünün piyasaya sürülmesinden bu yana bu saldırının neden olduğu hiçbir hasar raporu yoktur.

■ Karşı Önlemler

Bir hedef sürümü kullanıyorsanız lütfen donanım yazılımını [Yazılım ve Belgeler](#) bölümünden indirin ve hedef ürünü güncelleyin.

■ Sorularınız için irtibat

Hedef bir ürün kullanan bir müşteriyseniz ve bu konuyla ilgili herhangi bir sorunuz varsa, lütfen bizimle iletişime geçmekten çekinmeyin. Sağladığınız e-posta adresi üzerinden sizinle iletişim kuracağız.

►Bizimle iletişime geçin

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

Müşteri tarafından sağlanan kişisel bilgiler, bu husus dışında başka bir amaç için kullanılmayacaktır.

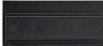
Lütfen gizlilik politikamız için <https://www.aiphone.net/privacy/> adresini kontrol edin.

■ Referans bilgileri

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

16 Ekim 2024
AIPHONE CO., LTD.

O Hedef Ürünler Listesi

Ürün Adı	Model No.	Ürün Görüntüsü	CVE-2024-31408, CVE-2024-39290		CVE-2024-47142		CVE-2024-45837	
			Önlemler öncesi sürüm	Önlemler sonrası sürüm	Önlemler öncesi sürüm	Önlemler sonrası sürüm	Önlemler öncesi sürüm	Önlemler sonrası sürüm
Kıracı İstasyonu	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
Giriş İstasyonu	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
Koruma İstasyonu	IXG-MK	 IXG-MK	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
Ağ Geçidi Adaptörü	IXGW-GW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
	IXGW-TGW		Ver3.01	Ver4.00	-	-	Ver3.01	Ver4.00
Asansör Kont. Adaptörü	IXGW-LC	 IXGW-LC	Ver3.00	Ver4.00	-	-	Ver3.00	Ver4.00
IXG Destek Aracı	-	-	-	-	-	-	Ver5.0.2.0	Ver6.0.0.0