

Aiphone Intercom System Vulnerability Allows Hackers to Open Doors

A vulnerability in Aiphone intercom products allows attackers to breach the entry system and gain access to the building that uses it.

Aiphone is one of the largest global manufacturers of intercom systems, including audio and video entry systems for residential and corporate buildings.

Last week, researchers with Norwegian application security firm Promon published information on a vulnerability identified in several Aiphone products that could allow an attacker to easily breach the entry system using an NFC tag.

The security bug is tracked as CVE-2022-40903 and is described as an information disclosure vulnerability.

The issue was identified in June 2021 and impacts Aiphone device series GT-DMB, GT-DMB-N, and GT-DMB-LVN running firmware versions prior to 3.00, and GT-DB-VN devices running firmware version 2.00 or earlier.

Promon says that the bug allows an attacker to “use a mobile device with NFC capability to run a brute-force attack on the entry system” in order to find the admin passcode”.

Essentially, the system allows an attacker with network access to try every possible four-digit code combination to discover the admin passcode, Promon said, responding to a SecurityWeek inquiry.

According to Promon, “the exploit requires a modification app (a custom Android NFC host-based emulation app that mimics the behavior of the official administrative tool).”

Once they know the administrator passcode, the attacker can use it to add a new NFC tag into the system (by injecting the device’s serial number), for access into the building.

This gives “the attacker both the code in plain text that can then be punched into the keypad, but also an NFC tag that can be used to gain access to the building without the need to touch any buttons at all”, the application security firm said.

Given that the vulnerable Aiphone products do not store access logs, an organization may be unaware of any unauthorized access, as there would be no evidence of it on the device.

“Unfortunately, there’s no way of knowing if a device has been targeted by this type of attack,” Promon said.

The main issue, however, is that the vulnerability cannot be addressed via a software update, requiring a hardware replacement instead.

On November 10, Aiphone published a vulnerability notification on its website, saying that device models manufactured after December 7, 2021 are no longer vulnerable and encouraging customers using older models to contact the vendor for instructions.

“Regarding the Video Multi-Tenant System Entrance Station GT-DMB-N, GT-DMB-LVN, and GT-DB-VN sold by Aiphone since their launch in June 2017, it has been found that there is a vulnerability in the Entrance Station that may lead to leakage of the settings information in the products or to partial loss of functionality. This attack requires a highly specialized technique,” the vendor says.

The vendor warns that an attacker may exploit the vulnerability to open doors without authorization, but says that it has received no reports of the vulnerability being exploited in attacks.