Open garage doors anywhere in the world by exploiting this “smart” device

Getty Images

reader comments

128 with

Share this story

A market-leading garage door controller is so riddled with severe security and privacy vulnerabilities that the researcher who discovered them is advising anyone using one to immediately disconnect it until they are fixed.

Each $80 device used to open and close garage doors and control home security alarms and smart power plugs employs the same easy-to-find universal password to communicate with Nexx servers. The controllers also broadcast the unencrypted email address, device ID, first name, and last initial corresponding to each one, along with the message required to open or shut a door or turn on or off a smart plug or schedule such a command for a later time.

Immediately unplug all Nexx devices

The result: Anyone with a moderate technical background can search Nexx servers for a given email address, device ID, or name and then issue commands to the associated controller. (Nexx controllers for home security alarms are susceptible to

a similar class of vulnerabilities.) Commands allow the opening of a door, turning off a device connected to a smart plug, or disarming an alarm. Worse still, over the past three months, personnel for Texas-based Nexx haven't responded to multiple private messages warning of the vulnerabilities.

"Nexx has consistently ignored communication attempts from myself, the Department of Homeland Security, and the media," the researcher who discovered the vulnerabilities wrote in a post published on Tuesday. "Device owners should immediately unplug all Nexx devices and create support tickets with the company requesting them to remediate the issue."

The researcher estimates that more than 40,000 devices, located in residential and commercial properties, are impacted and more than 20,000 individuals have active Nexx accounts.

Nexx controllers allow people to use their phones or voice assistants to open and close their garage doors, either on command or at scheduled times of the day. The devices can also be used to control home security alarms and smart plugs used to remotely turn on or off appliances. The hub of this system are servers operated by Nexx, which both the phone or voice assistant and garage door opener connect to. The five-step process for enrolling a new device looks like this:

Advertisement

1. The user uses the Nexx Home mobile app to register their new Nexx device with the Nexx Cloud.
2. Behind the scenes, the Nexx Cloud returns a password for the device to use for secure communications with the Nexx Cloud.
3. The password is transmitted to the user's phone and sent to the Nexx device using Bluetooth or Wi-Fi.
4. The Nexx device establishes an independent connection with the Nexx Cloud using the provided password.
5. The user can now operate their garage door remotely

using the Nexx Mobile App.

This is an illustration of the process:

Sam Sabetan

A universal password that’s easy to find

To make all of this work, the controllers use a lightweight protocol known as MQTT. Short for Message Queuing Telemetry Transport, it’s used in low-bandwidth, high-latency, or otherwise unstable networks to foster efficient and reliable communication between devices and cloud services. To do this, Nexx uses a publish-to-subscribe model, in which a single

message is sent between subscribed devices (the phone, voice assistant, and garage door opener) and a central broker (the Nexx cloud).

Researcher Sam Sabetan found that devices use the same password to communicate with the Nexx cloud. What's more, this password is easily attainable simply by analyzing the firmware shipped with the device or the back-and-forth communication between a device and the Nexx cloud.

"Using a universal password for all devices presents a significant vulnerability, as unauthorized users can access the entire ecosystem by obtaining the shared password," the researcher wrote. "In doing so, they could compromise not only the privacy but also the safety of Nexx's customers by controlling their garage doors without their consent."

When Sabetan used this password to access the server, he quickly found not only communications between his device and the cloud but communications for other Nexx devices and the cloud. That meant he could sift through the email addresses, last names, first initials, and device IDs of other users to identify customers based on unique information shared in these messages.

Advertisement
But it gets worse still. Sabetan could copy messages other users issued to open their doors and replay them at will—from anywhere in the world. That meant a simple cut-and-paste operation was enough to control any Nexx device no matter where he or it was located.

A proof-of-concept video demonstrating the hack follows:

[embedded content]
NexxHome Smart Garage Vulnerability – CVE-2023-1748.
This event brings to mind the worn-out cliché that the S in IoT—short for the umbrella term Internet of Things—stands for security. While many IoT devices provide convenience, a

frightening number of them are designed with minimal security protections. Outdated firmware with known vulnerabilities and the inability to update are typical, as are myriad flaws such as hardcoded credentials, authorization bypasses, and faulty authentication verification.

Anyone using a Nexx device should seriously consider disabling it and replacing it with something else, although the usefulness of this advice is limited since there’s no guarantee that the alternatives will be any safer.

With so many devices at risk, the US Cybersecurity and Infrastructure Security Agency issued an advisory that suggests users take defensive measures, including:

- Minimizing network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- Locating control system networks and remote devices behind firewalls and isolating them from business networks.
- When remote access is required, use secure methods, such as virtual private networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

Of course, those measures are impossible to deploy when using Nexx controllers, which brings us back to the overall insecurity of IoT and Sabetan’s advice to simply ditch the product unless or until a fix arrives.

https://arstechnica.com/?p=1929120