ALLEGION

Customer Bulletin

Date: May 2023

Security Advisory Regarding “Flipper Zero” Tool

Overview

Allegion has become aware of a tool called Flipper Zero, which is a portable multi-tool for pentesters that enables users to hack some digital products, such as radio protocols, access control systems, hardware and more. Flipper Zero has multiple communication channels including sub-1GHz, both low- and high-frequency RFID, infrared and Bluetooth. As a result, this tool can exploit vulnerabilities in less secure RFID credential technologies, potentially affecting a number of market verticals and institutions.

Security Findings

Under certain circumstances, the tool could be used to gain unauthorized access to rooms using a cloned or emulated RFID credential. More specifically, Flipper Zero can clone low frequency proximity credentials, high frequency credentials not employing encryption (MIFARE Ultralight and Ultralight C), and also be used to exploit an already known vulnerability with NXP MIFARE Classic (an RFID credential technology that contains an encryption algorithm that has been compromised). While compromises related to MIFARE Classic’s encryption have been published previously, with Flipper Zero, it is important to note the following:

- Cloning or hacking a MIFARE Classic credential does not reveal the default encryption key. The key is obfuscated by additional Allegion security methods to make it nearly impossible to decipher.
- Each hack is unique to a single credential. In other words, it cannot be used as a basis to then emulate a different card, unless it has the exact card to clone.

Allegion’s Cybersecurity Team continues to monitor Flipper Zero exploits; however, to date, research shows there is no threat of Flipper Zero exploiting MIFARE DESFire EV Series credentials, as it uses AES128 encryption, which has never been compromised.

Recommendation

While Allegion offers credentials providing various levels of security (based on customers’ / users’ unique needs), we also continue to recommend using a higher level of security than what is provided with MIFARE Classic. Upgrade solutions (more secure credentials) are available utilizing a user’s existing multi-technology reader and locking hardware platforms. Consult your Allegion Sales Representative to discuss upgrade options.

As a leading global security solutions provider, we take any potential vulnerabilities impacting our industry and our products very seriously. Our products are continually evolving to stay on the leading edge of protecting against potential threats. With this in mind, we also encourage all customers with electronic or connected hardware to stay up-to-date with the latest security measures and software/firmware.

Contact Us

For additional information on this topic, please contact: cybersecurity@allegion.com