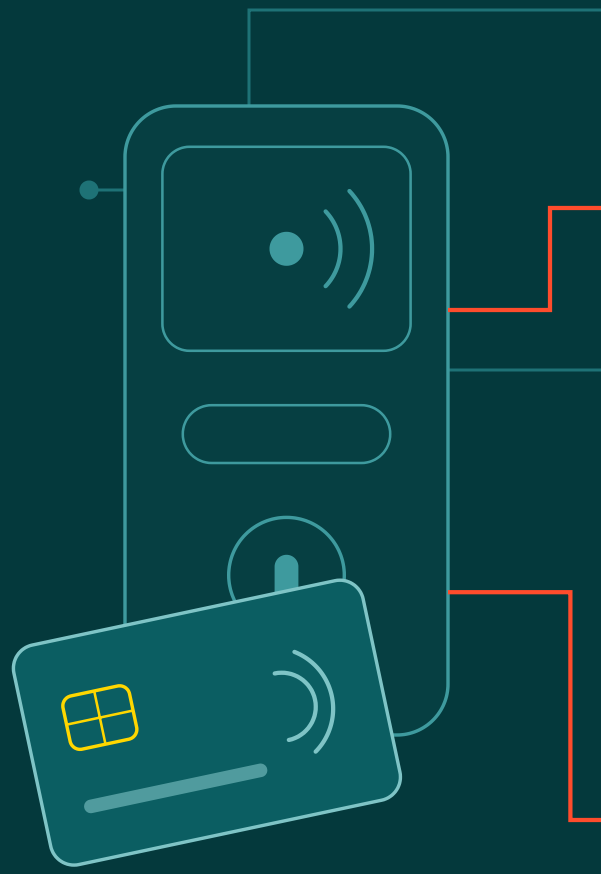
CASE STUDY

CS-2026-01

ioSENTRIX

Your Trusted Partner in Cybersecurity



IOT AND EMBEDDED DEVICE SECURITY

How a copied card ID could open a connected lock

A flawed card check fell back to a copyable ID, and an opened enclosure gave a second, silent way in.

CLIENT
Connected-device maker

SERVICE
IoT and embedded device penetration testing

ENGAGEMENT
Multi-week, fixes in 30 days

VERIFIED
Every fix retested by ioSENTRIX

AT A GLANCE

CLIENT
Connected-device maker

PRODUCT
Connected lock with card access and a cloud portal

DRIVER
Product launch and a customer requirement

SERVICE
IoT and embedded device penetration testing

SCOPE
Boards and enclosure, firmware, card reader, wired interfaces, OTA updates

ACCESS
Firmware source and production binaries; no debug build

ENGAGEMENT
A multi-week engagement; fixes rolled out within 30 days

VERIFIED
Every fix retested by ioSENTRIX

TESTED BY
ioSENTRIX hardware and firmware testers

EXECUTIVE SUMMARY

Two ways to open the lock without a trace, both closed and verified

A connected-device maker needed an attacker's view of its lock before launch, both for its own release and because a customer required independent testing. Over a multi-week engagement, ioSENTRIX tested the device from the circuit board to the update channel.

We found that a copied card ID could open the door, and that anyone inside the enclosure could open it with nothing logged. The client rolled out fixes for every finding within 30 days, and ioSENTRIX retested each one.

10+	30	100%
findings, 2 of them High severity	days for the client to roll out every fix	of fixes verified by ioSENTRIX retest

The encryption was sound. The way in was what the lock did when encryption failed.

Details in this case study are anonymised and generalised. Methods that could harm other products are withheld.

© 2026 ioSENTRIX LLC

01 What we found

HIGH FINDING 1

A copied card ID was enough to open the door

The firmware's check for the expected card application used a bitwise OR, so every card passed it. When the MIFARE DESFire cryptographic step then failed, the firmware fell back to the card's UID alone, an identifier read before any key is used.[1]

Business impact: card entry, the product's core promise, could be defeated with a copied identifier instead of a stolen card.

MEDIUM FINDING 2

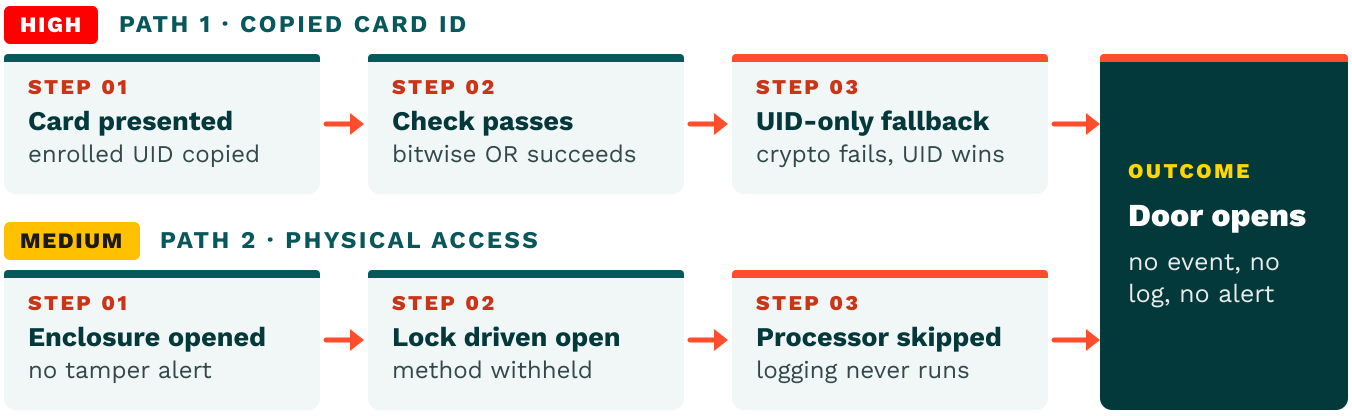
Opening the enclosure gave a second, silent way in

There was no tamper detection. Inside, our testers found ways to drive the lock open directly, bypassing its processor, so no unlock event, log entry or alert reached the portal.

Business impact: a break-in by this route would leave no trace, for the customer or the maker.

Please note: the physical bypass methods are deliberately withheld from this publication.

Figure 1. Two separate paths to an unlocked door, neither of them logged



HOW WE FOUND IT

These were logic flaws on a failure path, not known vulnerabilities, so an automated scanner had nothing to match them against. Finding them took reading the firmware source against the production binary and testing the hardware by hand.

[1] NXP Semiconductors, AN10927 "MIFARE product and handling of UIDs", Rev. 4.1, 2018.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. Findings by severity (10+ findings)[2]



Also found: a stack overflow on long card UIDs, UID cloning on legacy cards, a flash-read overflow, build paths in the binary and missing NULL checks in update handlers.

WHAT CHANGED

All fixes rolled out within 30 days · verified by ioSENTRIX retest

- **Card authentication.** The application check compares correctly; the UID-only fallback is gone.
- **Memory safety.** UIDs and flash reads are length-checked; update handlers check for NULL.
- **Physical bypass.** The lock detects movement it did not command; tamper sensors alert the portal.
- **Release hygiene.** Build paths no longer ship in the firmware binary.

03 Lessons for device makers

Test the failure path

The encryption was sound. The fallback was the way in.

A UID is not a credential

It identifies a card. It does not prove the card is genuine.

Expect the enclosure to open

Limit exposed interfaces and watch telemetry (ETSI EN 303 645, 5.6-3 and 5.10-1).[3]

[2] Severity rated on a five-level likelihood and impact matrix based on NIST SP 800-30 Rev. 1.

[3] ETSI EN 303 645 V2.1.1 (2020-06), cited as alignment guidance, not a compliance claim.

ioSENTRIX

Planning a device release? See a sample IoT test report or book a strategy session on your hardware, firmware and cloud.

iosentrix.com/contact-us

contact@iosentrix.com

+1 (888) 958-0554

13800 Coppermine Rd, Suite 190
Herndon, VA 20171

CREST-accredited · ISO/IEC 27001 certified · SOC 2 Type 2 attested

© 2026 ioSENTRIX LLC. General information only. Client details anonymised.