CASE STUDY

CS-2026-06

ioSENTRIX

Your Trusted Partner in Cybersecurity



IOT AND GUEST-TECHNOLOGY SECURITY

How a guest tablet could control other rooms at a hospitality company

A black-box test of an in-room automation system found a path from one guest's tablet to staff systems.

CLIENT
Hospitality company

SERVICE
IoT and network penetration testing

APPROACH
Black-box, no inside information

VERIFIED
Critical and High fixed; retested by ioSENTRIX

AT A GLANCE

CLIENT
Hospitality company

PRODUCT
In-room automation system run from a guest tablet

SERVICE
IoT and embedded device penetration testing

SCOPE
Guest tablet, room automation system and its network connections

ACCESS
Black-box: no source code or system details

VERIFIED
Critical and High fixed; retested by ioSENTRIX

TESTED BY
ioSENTRIX IoT and network testers

EXECUTIVE SUMMARY

One guest tablet reached other rooms, room service and the network behind them

A hospitality company was rolling out an in-room tablet that let guests control temperature, curtains, entertainment, room service and their bill. It asked ioSENTRIX to test the system the way a guest with bad intentions would, with no inside information.

We found that a guest could control devices in other rooms, place orders that were not theirs, and move from the room system towards the network that runs billing. The client remediated the findings, and ioSENTRIX retested the fixes.

20+	3	0
findings, 3 of them Critical	ways to reach beyond the guest's own room	guest features lost to the fixes

One room's tablet could reach every other room, and the network behind them.

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

© 2026 ioSENTRIX LLC

01 What we found

THEME · ACCESS CONTROL FINDING 1

A guest could control other rooms

Weak password policies allowed simple, predictable passwords on the room automation system. From one in-room tablet, our testers could change temperature, curtains and TVs in other guests' rooms and place room-service orders that were not their own.

Business impact: guests in any room could be disturbed or billed for orders they never made.

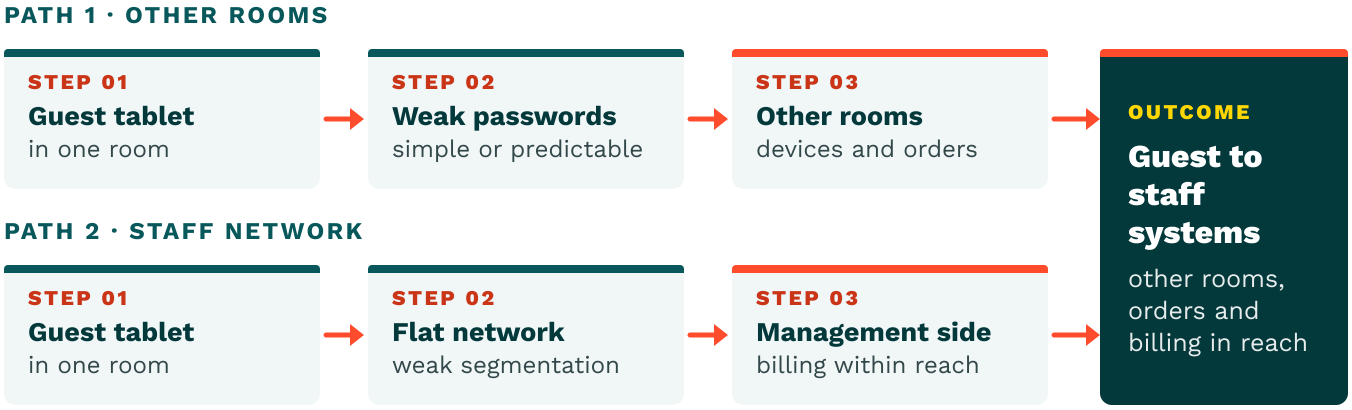
THEME · SEGMENTATION FINDING 2

The room system could reach staff networks

The room automation network was not separated enough from the hotel's management networks. From the guest side, a path existed onto the network that hosts the billing system.

Business impact: a guest-facing device could become a way into financial and operational systems.

Figure 1. Two paths from a single guest tablet



HOW WE FOUND IT Testing started with nothing but a guest's tablet, no source code or system details, and worked outwards: first the room system, then other rooms, then the network behind them.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. Findings by severity (20+ findings)



Figure 3. What changed

Critical and High fixed by the client; retested by ioSENTRIX

AREA	BEFORE THE TEST	AFTER REMEDIATION
Room-to-room control	Predictable passwords let one guest tablet control other rooms' temperature, curtains and TVs	● Stronger password policies and security configuration on the room system
Room service	Orders could be placed for rooms that were not the guest's own	● Remediated with the room system fixes
Network separation	A path ran from the room network towards billing	● Room automation network segmented from the hotel's management networks

03 Lessons for hospitality teams

Treat guest devices as hostile

One tablet with predictable passwords reached other rooms. Unique credentials and per-room authorisation keep guests in their own room.

Finding 1 · OWASP IoT Top 10 (2018), I1: Weak, Guessable, or Hardcoded Passwords

Keep guests off the back office

The room network had a route towards billing. Guest systems need their own segment, with no path to finance.

Finding 2

Test it as a guest would

A black-box test shows what someone staying one night can reach, before a real guest finds out.

Approach

ioSENTRIX

Rolling out guest-facing technology? See a sample IoT test report or book a strategy session before it reaches every room.

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.