Breaking the Alarm: Vulnerability Disclosure of the D3D Wi-Fi Security System (433 MHz Replay Attack)

The D3D ZX-G12 is a widely marketed Wi-Fi alarm system used across homes and small offices. It pairs with wireless door sensors, PIR motion detectors, and sirens using the 433 MHz ISM band, a low-cost RF spectrum common in consumer IoT devices.

During a wireless security assessment, I discovered a critical flaw in the system's RF design:
The communication channel lacks essential security protections, making it vulnerable to RF replay attacks capable of spoofing or manipulating sensor events.

This disclosure follows responsible practices, and the issue has been submitted to MITRE for CVE assignment.

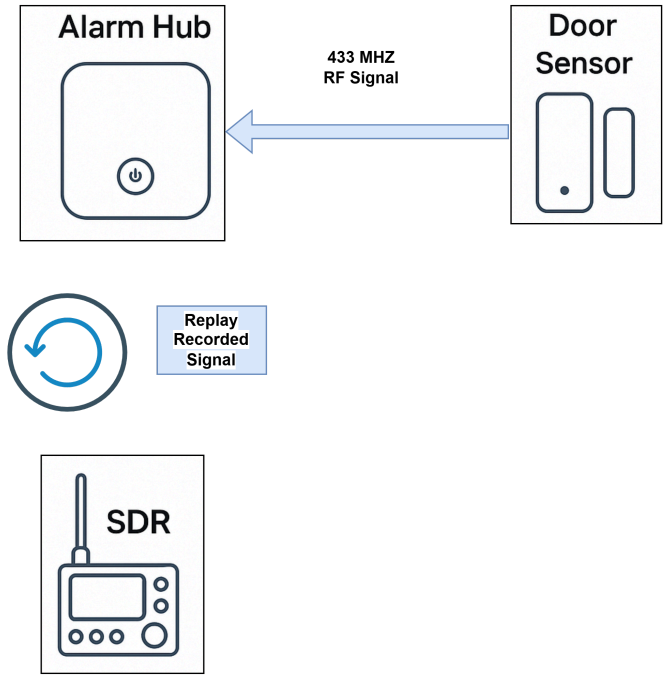
Vulnerability Summary

The 433 MHz sensors transmit static, unencrypted, and unauthenticated RF packets.The alarm hub accepts any transmission matching a known sensor ID, without validating:

1. Freshness
2. Authenticity
3. Replay attempts
4. Source integrity

An attacker within RF range can record a legitimate sensor transmission and later replay it, forcing the hub to register a fake event (trigger or reset).

This weakness is classified as a Wireless Replay Attack.



Communication Design
The system's RF architecture is simple, but inherently insecure.

Alarm Hub
Receives RF frames, interprets sensor events, and communicates with the mobile app via Wi-Fi.

433 MHz RF Sensors
Door/PIR sensors transmit ASK/OOK-modulated frames at 433.30 MHz upon state changes.

Receiver Module
A low-cost fixed-code RF receiver that accepts any frame matching a stored pattern

Missing Security Components

1. No encryption
2. No rolling code / hopping code
3. No message authentication
4. No nonce / timestamp / sequence checks
5. No tamper detection

This creates a perfect environment for replay attacks.

Methodology

To analyze the RF communication, I performed a non-intrusive, over-the-air assessment focused solely on signal behavior.

Hardware

1. HackRF One
2. 433 MHz ISM-tuned antenna
3. Laptop running Kali

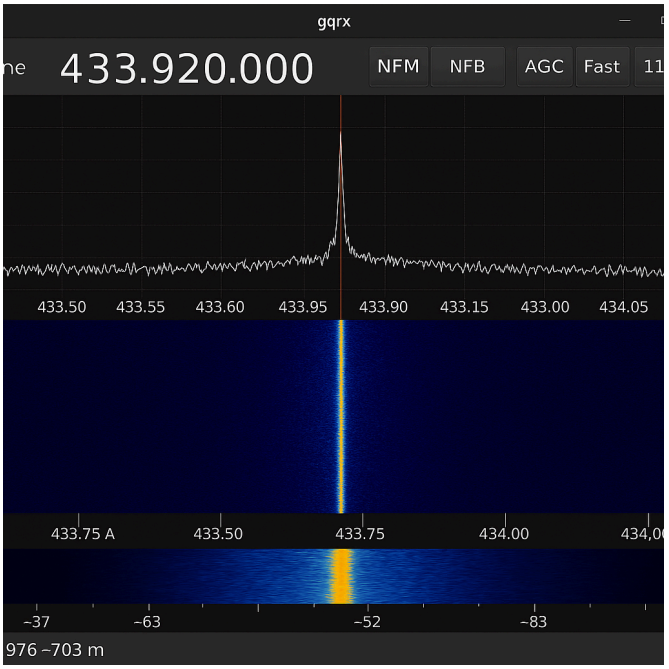
Software

1. GQRX – RF spectrum visualisation
2. GNU Radio Companion – waveform and protocol analysis

Testing Approach

1. Triggered door and PIR sensors to capture their RF emissions.
2. Analyzed waveform pulses and symbol structure.
3. Checked whether repeated transmissions varied (they did not).
4. Replayed captured frames to test the hub's response.

Every transmission produced the same static fixed-code pattern, confirming a complete absence of anti-replay design.



Findings

1.Static, Fixed-Code Packets

Each sensor emits a pulse train representing a constant binary ID.

Observations:

1. Frames never change
2. No counters, randomness, or freshness markers
3. Identical waveform on every activation

2.No Authentication or Rolling Code

The hub only checks:“Does this bit-pattern match a paired sensor?”

There is no protection against:

1. Replay
2. Cloning
3. tampering

3.Replay Behavior

Replaying a previously captured frame yielded:

1. Immediate acceptance by the hub
2. Log entry identical to real sensor activity
3. Alarm behavior (trigger/reset) identical to genuine transmissions

4.Highly Reproducible

Replay attacks succeeded:

1. across different sensors
2. at different times

Proof of Concept (PoC)

Tools

- HackRF
- GQRX
- GNU Radio Companion

PoC Flow

1. Recorded a legitimate 433 MHz door sensor activation
2. Replayed the captured waveform back at the same frequency
3. The hub interpreted the replay as a real event

This confirmed:

1. No anti-replay protection
2. Codes are cloneable
3. Sensor states can be spoofed without physical access

No firmware modification, Wi-Fi access, or app tampering was required.

Affected Models

D3D ZX-G12 Alarm Hub

433 MHz PIR Motion Detector

433 MHz Door/Window Sensor

Recommendations

For Users:

1. Avoid relying on unencrypted RF sensors for high-security needs
2. Prefer systems using rolling-code communication
3. Monitor for abnormal or repeated sensor triggers

For Vendors:

1. Implement rolling codes
2. Add cryptographic message authentication (MAC)
3. Use nonces, timestamps, or sequence counters
4. Adopt secure RF chipsets and modern IoT security standards

Conclusion

RF protocols continue to be a major weak point in consumer IoT products.The D3D ZX-G12 replay vulnerability demonstrates how the lack of authentication and freshness checks can compromise an entire security system.

Disclaimer

All testing was performed on devices owned by me, and within a controlled environment. I contacted the vendor to report the vulnerability, but did not receive any response despite multiple attempts. The vulnerability details have been submitted to MITRE for CVE assignment in line with responsible disclosure practices.

This article is published to help improve IoT security awareness. No exploitation was conducted beyond benign RF replay testing.