EXECUTIVE SUMMARY

SUMMARY

During the test, I was able to exploit the improper enforcement of behavioral workflow vulnerability. By exploiting the vulnerability, I was able to bypass the IP camera and gain access to the car.

This issue could allow an attacker to potentially generating interference on the camera's operating frequency, can prevent communication, rendering the camera temporarily "blind".

CONCLUSIONS

From my professional perspective, the overall security level of the system has remained **High.**

The tested environment was deficient in enforcement of behavioral workflow and secure session configuration implementation, with the main explanation vectors based on the following:

- Signal Jamming

-Unencrypted Communication

The exploitation of these vulnerabilities requires **low level** technical knowledge.

VULN-001 Unsecured communication(critical)

DESCRIPTION

The unsecured communication vulnerability is type of network-based attack where an attacker intercepts and captures legitimate data transmissions and then retransmits them at a later time to impersonate the sender or deceive the recipient.

An attacker can often exploit vulnerabilities in network communication where session integrity is not fully validated.
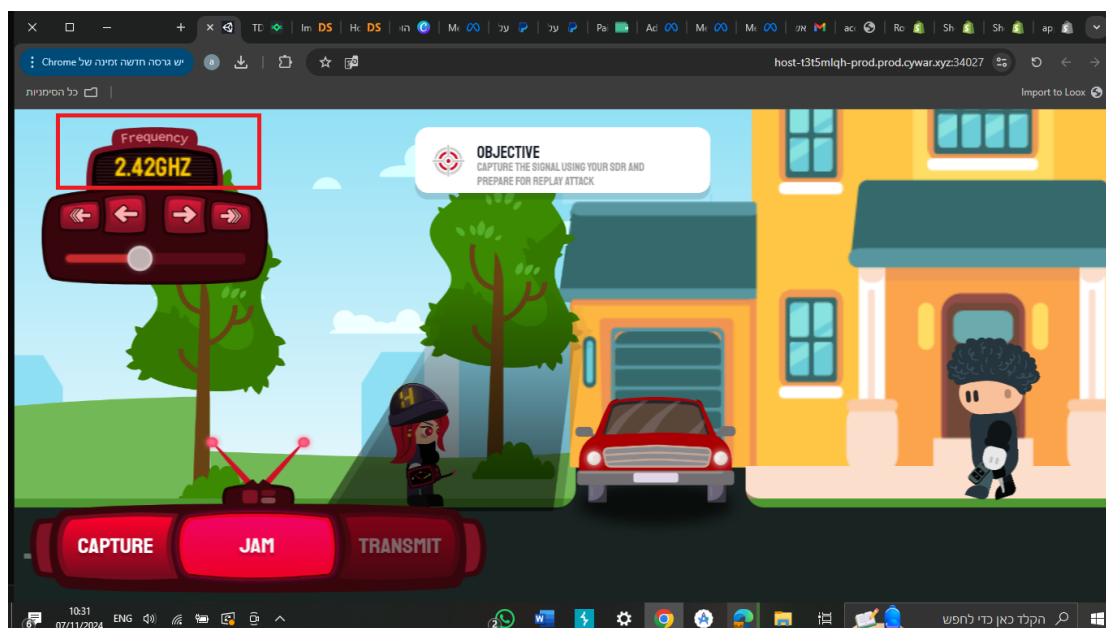
DETAILS

During the test I noticed that with the correct frequency I can gain access to the car.
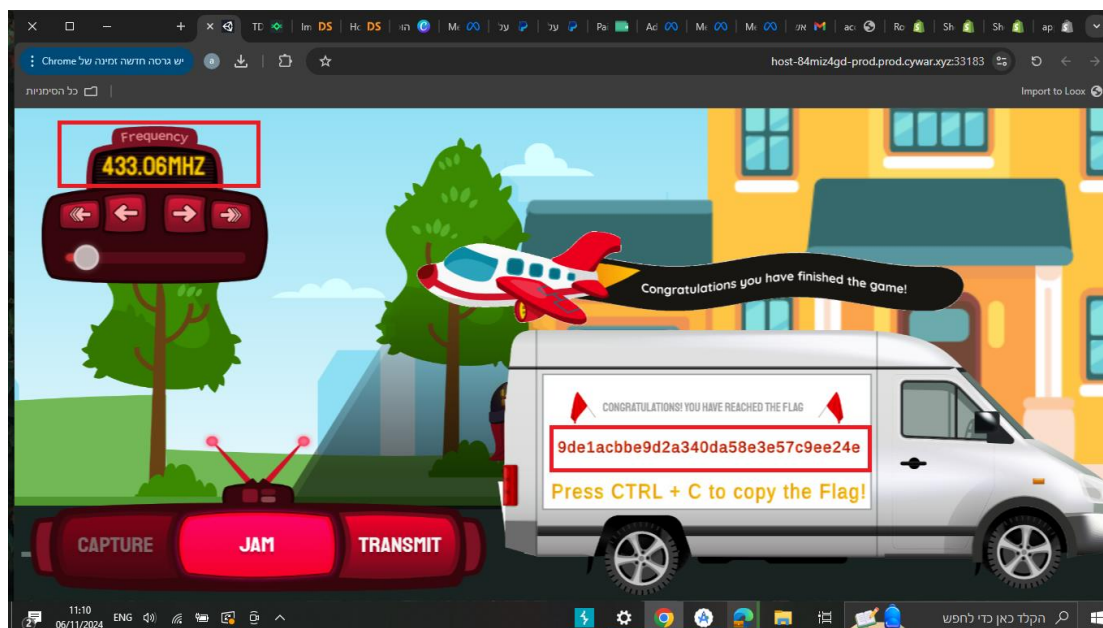
An attacker can potentially intercepts and captures legitimate data transmissions and .

EVIDENCE

Identification of the vulnerability was achieved by changing to the correct frequency and then capture the signal to gain access.

I changed to the common frequency and captured the signal

REMEDIATION OPTIONS

- TLS/SSL: Encrypting communications with Transport Layer Security (TLS) or Secure Sockets Layer (SSL) provides confidentiality and integrity, reducing the risk of interception and replay.

- Session Tokens : Securely exchanging session tokens that are invalidated after a single use or after a specific time frame.

FINDING DETAILS

VULN-002 Signal Jamming (High)

Description

In real world scenarios, many wireless IP cameras use Wi-Fi(2.4 GHz or 5 GHz frequencies) to transmit data. Signal Jamming is a situation where I can interfere with these transmissions, effectively disrupting the camera's ability to send video feeds or alerts to its monitoring system.

An attacker can exploit this vulnerability to effectively leave areas unmonitored and may prevent the camera from recording critical footage.

DETAILS

During the test, I discovered that with the correct frequency I can bypass the IP camera without providing any authentication details.

An attacker can exploit this vulnerability to prevent the camera ability alerts to its monitoring system, also can prevent the camera from recording critical areas.
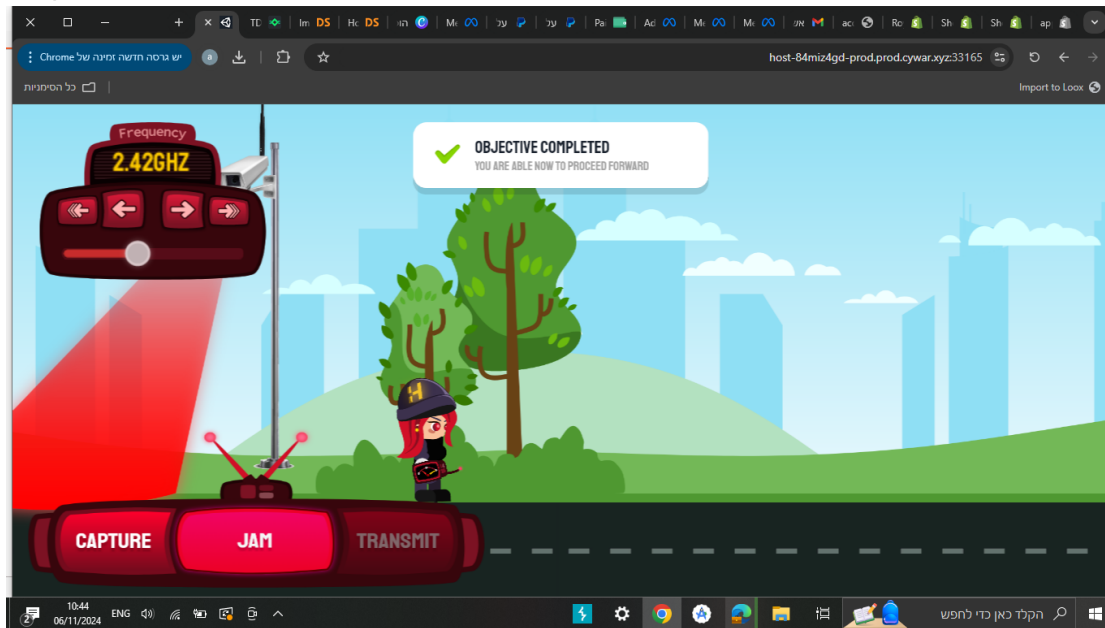
EVIDENCE

This vulnerability was identified while I noticed that with the right frequency I can avoid detection from the camera security, and bypass with anyone see me.
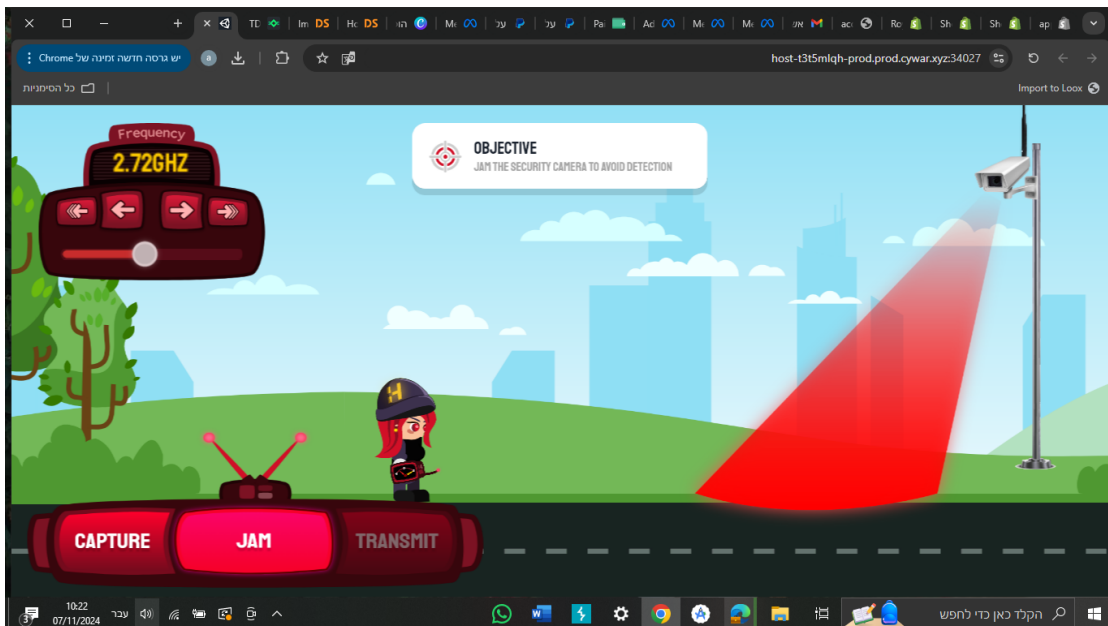
With the right frequency it can prevent detection from the camera
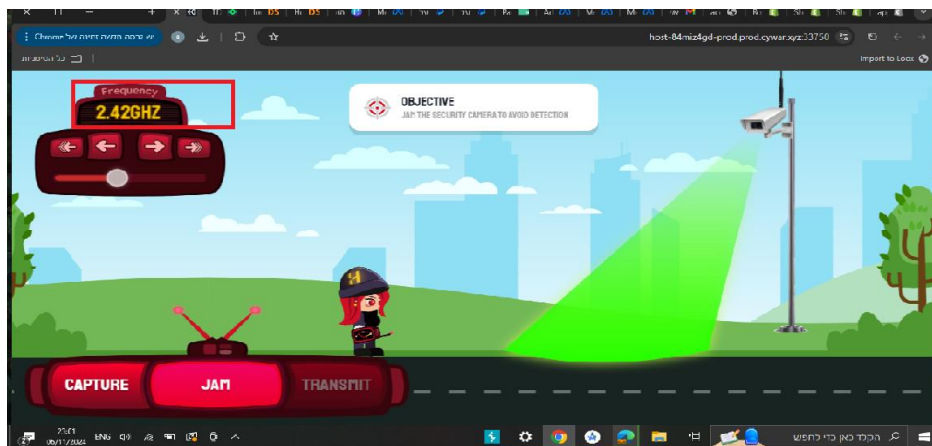
I passed the camera without detection

REMEDIATION OPTIONS

- Use Wired Connections: When possible, use Ethernet connections rather than relying solely on wireless.

- Detect Jamming : Advanced security system can detect abnormal levels of interference and issue alerts when jamming is suspected.