“Passive OSINT Reconnaissance on cruzio.com”

# Objective

using passive OSINT to gather intelligence on a target company without directly interacting with their systems. To get public information.

# Scope

**Target:** cruzio.com

**Techniques:** Shodan, DNSdumpster, prospeo.io, Data Aggregators & Public Records.

**No Active Scanning** — All data obtained from public sources.

# Methodology & Findings

## Step 1: Shodan

**Purpose:** finding domain name and vulnerabilities.

## Example Results:

* 1. Domain name: cruzio.com
  2. (21) critical vulnerabilities & (41) high vulnerabilities.

**Risk:** Data exfiltration & Denial of service & Huge reputation damage.

## Step 2: DNSdumpster

**Findings:** more than 500 subdomains.

## Step 3: prospeo.io

**Findings:** more than 800 emails with many breaches.

## Step 4: Data Aggregators & Public Records Sources Used:

HaveIBeenPwned:

* + - * [guru@cruzio.com](mailto:guru@cruzio.com) appeared in 20 breaches.
      * [keeper@cruzio.com](mailto:keeper@cruzio.com) appeared in 17 breaches.
      * [nivek@cruzio.com](mailto:nivek@cruzio.com) appeared in 17 breaches.
      * [dcdesign@cruzio.com](mailto:dcdesign@cruzio.com) appeared in 13 breaches.
      * [jaroyan@cruzio.com](mailto:jaroyan@cruzio.com) appeared in 7 breaches.
      * [bes@cruzio.com](mailto:bes@cruzio.com) appeared in 3 breaches.
      * [forestlakes@cruzio.com](mailto:forestlakes@cruzio.com) appeared in 2 breaches.

Shodan :

* + - * **(CVSS 10.0):** Apache Log4j 2.x before 2.16.0 allows remote code execution via JNDI lookups.
      * **(CVSS 9.8):** Go-based net/http (Golang) before 1.18.10 allows unauthenticated remote code execution via HTTP/2 streams.
      * **(CVSS 8.8):** Heap buffer overflow in WebP decoding (libwebp) allows remote code execution in browsers like Chrome.

# Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Example Finding** | **Potential Risk** | |
| Infrastructure | Apache Log4j 2.x before 2.16.0 | | remote code execution | |
| Infrastructure | Go-based net/http before 1.18.10 | | remote code execution | |
| Infrastructure | Heap buffer overflow in WebP | remote code execution | |
| Credentials | Breached email/password combo | Account takeover risk | |

1. **Recommendations**
   1. Apply WHOIS privacy protection.
   2. Regularly monitor for leaked credentials.
   3. Apply patches and updates for all outdated and vulnerable   
        
        
      **Note**: You can find out detailed information about subdomains and emails in the attached text file.