

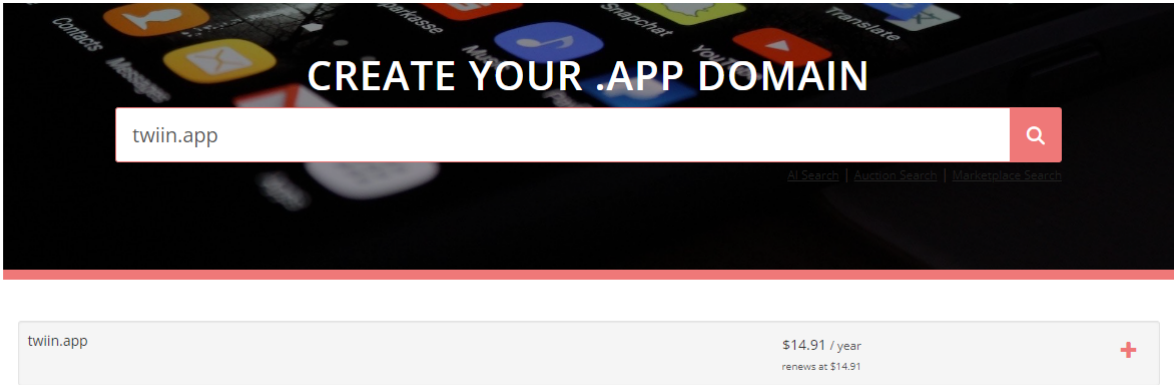
Identified Vulnerable Domain Names

This document presents examples of identified vulnerable domain names to demonstrate the validity and feasibility of our findings. We disclose only domains that were previously vulnerable but have since been resolved, minimizing real-world impact and preventing potential exploitation by malicious parties.

In some instances, we include screenshots taken during testing to verify domain statuses that can no longer be reproduced.

Case 1: twiin.app (relic domain)

1. The domain name can be registered from a domain registrar.



2. The domain name has a delegation record in the TLD zone file.

```
ubuntu@VM-0-10-ubuntu:~$ dig twiin.app @ns-tld5.charlestonroadregistry.com.

; <<>> Dig 9.18.12-0ubuntu0.22.04.3-Ubuntu <<>> twiin.app @ns-tld5.charlestonroadregistry.com.
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 32260
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; COOKIE: 68d2fc8d42d4ffa30159933674030e536ed101df9964efe78d9479e8c5 (good)
;; QUESTION SECTION:
;twiin.app.                IN      A

;; AUTHORITY SECTION:
twiin.app.                 10000   IN      NS      ns-cloud-a3.googledomains.com.
twiin.app.                 10000   IN      NS      ns-cloud-a2.googledomains.com.
twiin.app.                 10000   IN      NS      ns-cloud-a4.googledomains.com.
twiin.app.                 10000   IN      NS      ns-cloud-a1.googledomains.com.
```

3. The domain name does not have a WHOIS record.

ICANN | LOOKUP

Registration data lookup tool

Enter a [domain name](#) or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

twiin.app

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [registration data lookup tool Terms of Use](#).

For additional information on ICANN Accredited Registrars including website and contact information, please visit <https://www.icann.org/en/accredited-registrars>.

If the registration data you are seeking is not provided in the lookup results, please use the [Registration Data Request Service \(RDRS\)](#) to submit a request for nonpublic registration data. RDRS is intended for use by requestors with a legitimate interest in accessing nonpublic registration data.

The requested domain was not found in the Registry or Registrar's RDAP server.

4. Attackers can take over the domain name through the delegation records in the TLD name servers, which allows them to abuse an unregistered domain name.
5. We reported the issues to the backend registry, Nomulus (Google), and they have been successfully resolved.



Lai Jiang <jianglai@msn.com>



收件人: Jingkai Yu

周二 2025/1/21 20:58

抄送: 你

Hi Jingkai,

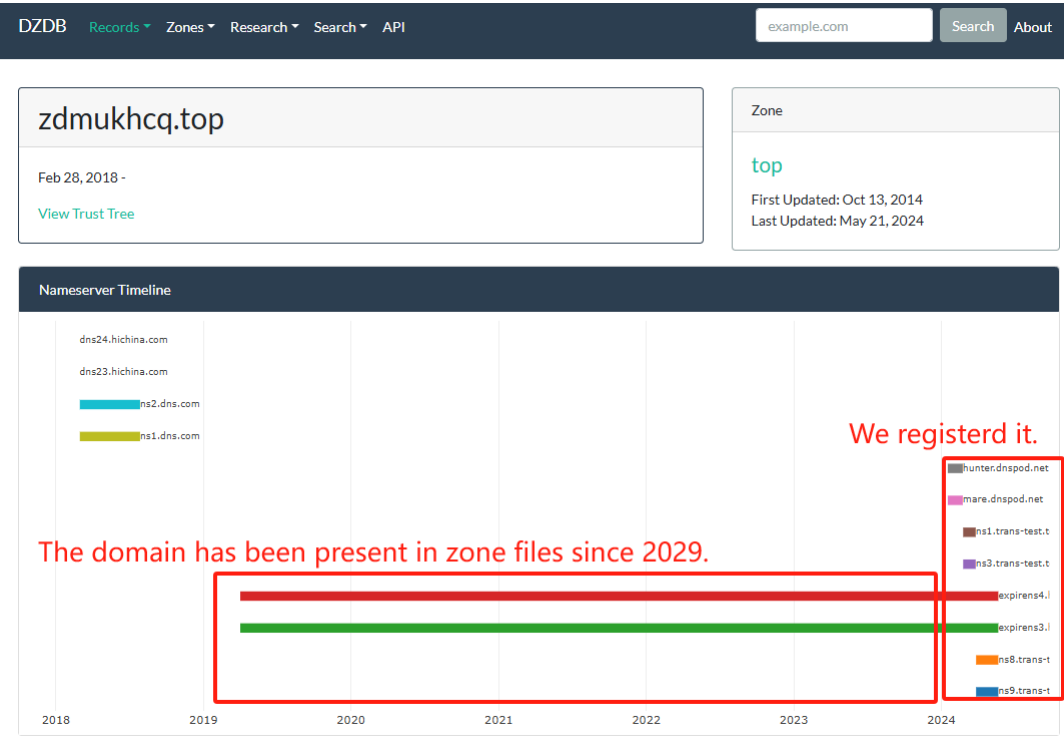
Thank you for reaching out prior to publication. We appreciate it. I checked our bug tracking system and it appears to be fixed. I am double checking with the person responsible to make sure that is indeed the case and will get back to you shortly.

Best,
Lai

Case 2: zdmukhcq.top (relic domain)

This domain encountered the same issue as Case 1.

1. The domain has been present in zone files since 2019, which can be found in [DNS coffee](#). After we found this issue, we registerd it.



2. Now, this issue has been addressed by the backend registry, ZDNS.

Case3: xn--86q281bo5hh1b.cn (twin domain)

1. The xn--86q281bo5hh1b.cn (冒泡游戏.cn) and xn--86qv51bo8hhkb.cn (冒泡游戏.cn) are a pair of twin domains. Among these IDNs, xn--86qv51bo8hhkb.cn (冒泡游戏.cn) was registered by a registrant and xn--86q281bo5hh1b.cn (冒泡游戏.cn) was created by the registry.
2. They have the same WHOIS record, with the Name Server set to DNSPod.

```
status:      ACTIVE
remarks:     Registration information: http://www.cnnic.cn/

created:     1990-11-28
changed:     2018-03-01
source:      IANA

# whois.cnnic.cn

Domain Name: 冒泡游戏.cn
Puny Name: xn--86q281bo5hh1b.cn
Domain Name: 冒泡游戏.cn
Puny Name: xn--86qv51bo8hhkb.cn
ROID: 20201231s12345s16686384-cn
Domain Status: ok
Registrant: 益阳市赫山区银意百货店
Registrant Contact Email: 13267383755@163.com
Sponsoring Registrar: 广州云讯信息科技有限公司
Name Server: cube.dnspod.net
Name Server: guanaco.dnspod.net
Registration Time: 2020-12-31 16:07:21
Expiration Time: 2021-12-31 16:07:21
DNSSEC: unsigned
```

- Customers assigned the same NS domains (i.e., *cube.dnspod.net* and *guanaco.dnspod.net*) can configure *xn--86q281bo5hh1b.cn* (冒泡游戏.cn) on their configuration pages. (Note: The domain was added solely for testing purposes, without configuring any DNS resource records for malicious use.)

