

Instantly share code, notes, and snippets.

minanagehsalalma / [ZTE ZXHN router vulnerabilities.md](#)



Created 2 months ago

<> **Code** ↻ Revisions 1

ZTE ZXHN router vulnerabilities – CVE-2026-34472, CVE-2026-34473, CVE-2026-34474

[ZTE ZXHN router vulnerabilities.md](#)

# ZTE ZXHN router vulnerabilities

Public disclosure date: 2026-03-27 Researcher: Mina Nageh Salama Zekry

This advisory documents three vulnerabilities affecting multiple ZTE ZXHN router models. The following CVE IDs were assigned by the CVE Program:

- CVE-2026-34472
- CVE-2026-34473
- CVE-2026-34474

## CVE-2026-34472 — ZXHN H188A V6.0 unauthenticated credential disclosure leading to authentication bypass

**Affected product:** ZTE ZXHN H188A V6.0

**Affected versions:** V6.0.10P2\_TE, V6.0.10P3N3\_TE

### Summary:

An unauthenticated user can access sensitive configuration data exposed by the web wizard interface, including administrative, WLAN, and PPPoE credentials. The issue can lead to information disclosure and unauthorized administrative access.

### Impact:

Information disclosure, authentication bypass, privilege escalation.

**Observed component / endpoint:**

```
/?_type=tedataNotLoginData&_tag=wizard_lua.lua&IF_ACTION=...
```

## CVE-2026-34473 — ZTE ZXHN H-series unauthenticated denial of service via oversized URL-encoded POST body

---

**Affected products / models include:**

H8102E, H168N, H167A, H199A, H288A, H198A, H267A, H267N, H268A, H388X, H196A, H369A, H268N, H208N, H367N, H181A, H196Q

**Affected version scope:**

Multiple firmware versions observed across affected H-series models, including versions in use prior to 2022.

**Summary:**

An unauthenticated attacker can send an oversized `application/x-www-form-urlencoded` POST request to the router management interface, causing the interface to become unresponsive.

**Impact:**

Denial of service / loss of availability of the management interface.

## CVE-2026-34474 — ZXHN H298A / H108N sensitive data exposure leading to credential leakage

---

**Affected products:**

ZTE ZXHN H298A, ZTE ZXHN H108N

**Affected versions:**

H298A V1.1, H108N V2.6

**Summary:**

Sensitive data is exposed through the web interface, allowing an unauthenticated user to obtain administrative credentials and WLAN-related secrets. The issue can enable unauthorized access and compromise of Wi-Fi credentials.

**Impact:**

Information disclosure, authentication bypass, privilege escalation.

### Observed component / endpoint:

`/getpage.lua?pid=1000&ETHCheat=1`

## Timeline

---

- 2024-05-02: Vulnerabilities reported to vendor
- 2026-03-27: CVE IDs assigned by the CVE Program