



Home > Submit > 782296

Submit #782296: Tenda AC10 V4 US_AC10V4.0si_V16.03.10.10_multi_TDE01 OS Command Injection

Title Tenda AC10 V4 US_AC10V4.0si_V16.03.10.10_multi_TDE01 OS Command Injection

Description An OS command injection vulnerability exists in the formAddMacfilterRule function in /bin/httpd of Tenda AC10 V4 firmware V16.03.10.10. User-controlled input from websGetVar() is passed to doSystemCmd() without adequate sanitization. Dataflow analysis confirms exploitable paths at 0x0044d47c and 0x0044d4a4. A total of 21 functions follow the same vulnerable pattern including formDelMacfilterRule, formSetFirewallCfg, formWifiApScan, and form_fast_setting_internet_set. An authenticated attacker can inject arbitrary OS commands resulting in root-level code execution.

Source <https://github.com/somanyerrors/tenda-ac10v4-vulnerabilities/blob/main/findings/CRITICAL-03-command-injection-formaddmacfilterrule.md>

User CoreNode (UID 96566)

Submission 03/18/2026 04:23 PM (18 days ago)

Moderation 04/04/2026 03:28 PM (17 days later)

Status Accepted

VulDB entry 355311 [Tenda AC10 16.03.10.10_multi_TDE01 /bin/httpd formAddMacfilterRule os command injection]

Points 20

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](#)