COMMUNITY CONTENT

Home › Submit › 782298

Submit #782298: Tenda AC10 V4 US_AC10V4.0si_V16.03.10.10_multi_TDE01 Cryptographic Issues

Title	Tenda AC10 V4 US_AC10V4.0si_V16.03.10.10_multi_TDE01 Cryptographic Issues
Description	An unencrypted RSA 2048-bit private key used by the httpd TLS server is stored in a web-accessible directory at /webroot_ro/pem/privkeySrv.pem in Tenda AC10 V4 firmware V16.03.10.10. The file is retrievable without authentication. An attacker can use the exposed key to decrypt all HTTPS traffic to and from the device, perform man-in-the-middle attacks, and capture admin credentials submitted via the login page. The corresponding certificate uses a deprecated SHA-1 signature and is self-signed, compounding the issue.
Source	https://github.com/somanyerrors/tenda-ac10v4-vulnerabilities/blob/main/findings/CRITICAL-05-exposed-rsa-private-key.md
User	CoreNode (UID 96566)
Submission	03/18/2026 04:34 PM (18 days ago)
Moderation	04/04/2026 03:28 PM (17 days later)
Status	Approved
VulDB entry	[Tenda AC10 16.03.10.10_multi_TDE01 RSA 2048-bit Private Key privkeySrv.pem hard-coded key]
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