
COMMUNITY
CONTENT

Submit #782053: Tenda 4G03 Pro V1.0 V04.03.01.53 Cryptographic Issues

Title	Tenda 4G03 Pro V1.0 V04.03.01.53 Cryptographic Issues
Description	Tenda 4G03 Pro V1.0 V04.03.01.53 Hardcoded ECDSA Private Key An unencrypted ECDSA P-256 private key is embedded in plaintext at /etc/www/pem/server.key in Tenda 4G03 Pro V1.0 firmware V04.03.01.53. The firmware image is publicly downloadable from the vendor website, meaning every attacker possesses the private TLS key for every deployed device worldwide. This enables decryption of all HTTPS traffic and man-in-the-middle attacks against any device running this firmware. Additional embedded keys found include /etc/www/pem/privkey_ima.pem and /etc/www/pem/privkey_evm.pem, which compromise the device firmware integrity verification chain. Proof: Download Link: https://www.tendacn.com/us/material/show/780447530344517 File /etc/www/pem/server.key confirmed present in publicly downloadable firmware image. Key type: ECDSA P-256 unencrypted PEM format. Full key material exposed. Firmware: US_4G03ProV1.0re_V04.03.01.53_multi_TDE01.bin SHA256: 21f12b93010376d89fde1872474c88d1f1e3553df9cdb14eed231d088f959022 Download: https://www.tendacn.com/us/material/show/73833207154694 9 Attack: Download firmware, extract server.key, use to decrypt HTTPS sessions or MITM any deployed device. Countermeasure: Generate unique key pairs per device at manufacturing or first boot. Never embed private keys in firmware images. Store keys in protected storage inaccessible from the filesystem.
User	CoreNode (UID 86586)
Submission	03/18/2026 03:29 AM (18 days ago)
Moderation	04/04/2026 08:20 AM (17 days later)
Status	Accepted
VulDB entry	[Tenda 4G03 Pro 1.0/1.0re/01.bin/04.03.01.53 ECDSA P-256 Private Key /etc/www/pem/server.key hard-coded key]
Points	17

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