INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-07 15:07 UTC

Tenda Router Firmware Carries Undocumented Admin Backdoor, CVE-2026-11405 Unpatched, No Vendor Fix Available

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0396
Type	CVE Vulnerability
CVE ID	CVE-2026-11405
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0024 (15th percentile)
Affected Products	Tenda router firmware: US_FH1201V1.0BR_V1.2.0.14(408)_EN_TD, US_W15EV1.0br_V15.11.0.5(1068_1567_841)_EN_TDE, US_AC10V1.0re_V15.03.06.46_multi_TDE01, US_AC5V1.0RTL_V15.03.06.48_multi_TDE01, US_AC6V2.0RTL_V15.03.06.51_multi_T
Published	2026-07-07T02:40:47
Discovery Source	Rss

Executive Summary

An undocumented authentication backdoor in multiple Tenda router firmware versions, tracked as CVE-2026-11405, has been reported to allow unauthenticated attacker access to administrative functions. Active exploitation is reported by security researchers but has not been confirmed by CISA KEV or a published CERT/CC advisory. No vendor patch is available and Tenda has issued no public response, leaving affected devices exposed until replaced or isolated. Organizations running affected Tenda router models on internet-facing networks face risk of unauthorized network access, traffic interception, and lateral movement into internal systems.

Technical Analysis

CVE-2026-11405 describes a hidden authentication bypass in the web server binary embedded in multiple Tenda router firmware versions, including US_FH1201V1.0BR_V1.2.0.14(408)_EN_TD, US_W15EV1.0br_V15.11.0.5(1068_1567_841)_EN_TDE, US_AC10V1.0re_V15.03.06.46_multi_TDE01, US_AC5V1.0RTL_V15.03.06.48_multi_TDE01, and US_AC6V2.0RTL_V15.03.06.51_multi_T. The vulnerability operates through a secondary code path that bypasses MD5 password verification, accepting any username

combined with a hidden configuration-stored password to grant full administrative access. Classified under CWE-912 (Hidden Functionality), CWE-259 (Use of Hard-coded Password), CWE-290 (Authentication Bypass by Spoofing), and CWE-287 (Improper Authentication), the flaw maps to MITRE ATT&CK techniques T1542.001 (Pre-OS Boot: System Firmware), T1133 (External Remote Services), T1040 (Network Sniffing), T1078 (Valid Accounts), T1556 (Modify Authentication Process), T1078.001 (Default Accounts), and T1098 (Account Manipulation). CVSS base score is 7.5 (High); EPSS score is 0.00243 (15th percentile) as of the source date. No patch exists. Active exploitation is reported by one T3 source (Rescana) but has not been confirmed by CISA KEV or a direct CERT/CC advisory in the provided source data. The NVD reference included in sources points to CVE-2026-56405, not CVE-2026-11405; that mismatch requires verification. All exploitation claims should be treated as reported but unconfirmed pending authoritative corroboration.

Action Checklist

1. Step 1: Containment. Immediately identify all Tenda router models running firmware versions US_FH1201V1.0BR_V1.2.0.14(408)_EN_TD, US_W15EV1.0br_V15.11.0.5(1068_1567_841)_EN_TDE, US_AC10V1.0re_V15.03.06.46_multi_TDE01, US_AC5V1.0RTL_V15.03.06.48_multi_TDE01, or US_AC6V2.0RTL_V15.03.06.51_multi_T (CIS 1.1). Block external access to the router web management interface (TCP 80/443/8080) at the network perimeter. Do not expose management interfaces to the internet. No vendor patch is available; isolation is the only containment measure at this time.
2. Step 2: Detection. Query firewall and web proxy logs for unexpected HTTP/HTTPS connections to router management interface ports from external IPs. Review router access logs (if retained) for authentication events using unexpected usernames or at unusual hours (NIST AU-6). Check for configuration changes to routing tables, DNS settings, or firewall rules that were not authorized (NIST CM-series). Review router access logs for unexpected account creation or privilege escalation events, if the device supports such logging. No confirmed IOC patterns are available from the provided source data.
3. Step 3: Eradication. No vendor-supplied firmware patch is available as of the source date. Until a patch is released by Tenda, replace affected router models with hardware running supported, patched firmware from an alternate vendor, or segment affected devices off network-critical paths. If replacement is not immediately possible, disable remote management interfaces and apply strict ACLs permitting management access only from dedicated administrator subnets (NIST AC-17, AC-6). Change all administrator credentials on affected devices as a precautionary measure; note that the underlying vulnerability may not be fully closed by credential rotation alone. Disable default accounts per CIS 4.7.
4. Step 4: Recovery. After isolation or replacement, verify that no unauthorized configuration changes persist: review routing tables, DNS forwarder settings, firewall rules, and administrator account lists. Confirm that management interface access is restricted to authorized management hosts only (NIST AC-3). Re-enable logging and alert on any future authentication attempts to management interfaces from unauthorized sources (NIST AU-2, AU-12, CIS 8.2). Monitor for lateral movement indicators in internal network traffic for 30 days post-remediation.
5. Step 5: Post-Incident. This vulnerability exposes a control gap in network hardware inventory and lifecycle management. Audit all network edge devices for end-of-support or unpatched firmware status (CIS 1.1, CIS 2.2, CIS 7.1). Establish a process to track vendor advisories for all network infrastructure hardware and to replace unsupported devices on a defined schedule (CIS 7.2). Review whether router management interfaces were internet-facing in violation of documented policy (NIST AC-17, AC-22). Consider adding network device firmware integrity monitoring to the detection program.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if forensic review of firewall or router logs confirms any successful unauthenticated HTTP 200 response to Tenda `/goform/` management endpoints from external IPs, or if DNS forwarder settings on the affected router were modified — either condition indicates active exploitation and potential data-path compromise requiring breach notification assessment under applicable regulations.
Recovery Notes	After replacing affected Tenda hardware, confirm the replacement device's DNS forwarder configuration matches the authorized baseline, as a successful CVE-2026-11405 exploitation could have silently redirected internal DNS resolution to an attacker-controlled resolver, potentially persisting as a credential-harvesting mechanism even after the router is isolated. Monitor internal DNS query logs and NetFlow/firewall logs for 30 days post-replacement for anomalous external DNS resolver usage or unexpected outbound connections from internal hosts that transited the compromised router. Do not return any previously affected network segment to full production trust without verifying that no downstream hosts show signs of having been redirected through attacker-controlled infrastructure during the exposure window.
Forensic Artifacts	Upstream firewall syslog records showing inbound TCP 80/443/8080 connections destined for affected Tenda management IP addresses from non-RFC1918 source addresses — the primary indicator of backdoor access attempts or success for CVE-2026-11405 | HTTP server access logs from the Tenda device (if syslog export was enabled) containing POST/GET requests to `/goform/` CGI endpoints — successful unauthenticated 200 responses to these paths are the direct forensic signature of backdoor invocation on affected firmware versions | Router running-configuration export captured before eradication, specifically the DNS forwarder table, static routing entries, and administrator account list — changes to any of these without corresponding authenticated admin sessions confirm post-exploitation activity | Packet capture (pcap) from a span port or inline tap on the upstream interface covering the exposure window, filtered for TCP sessions to/from the router management IP — provides ground-truth session reconstruction including whether the attacker issued configuration write commands via the backdoor | DHCP server lease logs from the affected router covering the full exposure window — identifies all internal clients that obtained network configuration (including potentially attacker-modified DNS server assignments) from the compromised device, defining the scope of downstream hosts requiring further triage

Per-Action IR Details

Step 1: Containment — Immediately identify all Tenda router models running firmware versions US_FH1201V1.0BR_V1.2.0.14(408)_EN_TD, US_W15EV1.0br_V15.11.0.5(1068_1567_841)_EN_TDE, US_AC10V1.0re_V15.03.06.46_multi_TDE01, US_AC5V1.0RTL_V15.03.06.48_multi_TDE01, or US_AC6V2.0RTL_V15.03.06.51_multi_T (CIS 1.1). Block external access to the router web management interface (TCP 80/443/8080) at the network perimeter. Do not expose management interfaces to the internet. No vendor patch is available; isolation is the only containment measure at this time.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST AC-4 (Information Flow Enforcement)

Compensating: Run `nmap -p 80,443,8080 --open ` to identify hosts responding on router management ports; cross-reference MAC OUI (Tenda OUI prefixes: C8:3A:35, C8:E7:D8, 00:26:5A) to confirm affected models. On the

upstream firewall or ISP router, insert explicit deny rules blocking inbound TCP 80/443/8080 destined for affected Tenda management IPs before making any further changes to the devices themselves.

Evidence: Before blocking perimeter access, capture: (1) current active TCP sessions to the router management interface using `netstat -ano` or `ss -tnp` on any monitoring host with visibility, (2) a full packet capture (Wireshark/tcpdump) on the upstream interface for at least 60 seconds to record any session already in progress, (3) router DHCP lease tables and ARP cache via the management interface if still accessible, documenting any unexpected client entries. These volatile connection-state artifacts will be destroyed the moment ACLs are applied.

Step 2: Detection — Query firewall and web proxy logs for unexpected HTTP/HTTPS connections to router management interface ports from external IPs. Review router access logs (if retained) for authentication events using unexpected usernames or at unusual hours (NIST AU-6). Check for configuration changes to routing tables, DNS settings, or firewall rules that were not authorized (NIST CM-series, no mapped control from knowledge base for config-change alerting specifically). Use D3-LAM (Local Account Monitoring) to identify unauthorized account creation or modification on affected devices. No confirmed IOC patterns are available from the provided source data.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Query upstream firewall syslog for inbound connections to Tenda management IPs on TCP 80/443/8080 from non-RFC1918 source addresses: `grep -E '(80|443|8080)' /var/log/firewall.log | grep -v '10\.|172\.1[6-9]\.|172\.2[0-9]\.|172\.3[01]\.|192\.168\.'`. If the Tenda device supports syslog export, capture authentication log lines; look for HTTP 200 responses to `/goform/` endpoints — the Tenda web UI CGI path — from external IPs, which would indicate successful backdoor invocation. Use Wireshark with display filter `tcp.port == 80 && http.request.uri contains "/goform/"` on a mirror/span port to catch live exploitation attempts.

Evidence: This step is observational and does not alter live state, so no volatile pre-capture is required before querying logs. However, if you identify an active session in progress, capture a full memory image of any internal host that communicated with the router management interface before terminating connections, and preserve raw pcap from the span port. Key artifacts to look for: HTTP GET/POST requests to Tenda-specific CGI paths (e.g., `/goform/setSysAdm`, `/goform/setUsbUnload`, `/goform/WizardHandle`) from external IPs, HTTP 200 response codes indicating successful unauthenticated access, and router syslog entries showing configuration write events without a preceding authenticated login event.

Step 3: Eradication — No vendor-supplied firmware patch is available as of the source date. Until a patch is released by Tenda, replace affected router models with hardware running supported, patched firmware from an alternate vendor, or segment affected devices off network-critical paths. If replacement is not immediately possible, disable remote management interfaces and apply strict ACLs permitting management access only from dedicated administrator subnets (NIST AC-17, AC-6). Change all administrator credentials on affected devices, recognizing that the hidden credential path may persist regardless of user-defined password changes (D3-CRO, D3-CH). Disable default accounts per CIS 4.7.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-17 (Remote Access), NIST AC-6 (Least Privilege), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Because the backdoor credential is hardcoded in firmware and user-defined password changes do not remove it, the only effective eradication for a team without budget for immediate hardware replacement is: (1) disable the web management service entirely via the router CLI if accessible (Tenda devices typically expose a limited shell; run `nvram set http_enable=0 && nvram commit`), (2) apply an upstream ACL permitting TCP 80/443/8080 only from a single dedicated management VLAN IP, and (3) document the device as formally untrustworthy in the asset inventory pending hardware replacement. Do not rely on credential rotation alone as a security control for

CVE-2026-11405.

Evidence: Before disabling the management interface or replacing hardware, capture: (1) a full router configuration export (running-config backup via the management UI or CLI `cfg -e` equivalent for Tenda firmware) to document the pre-eradication state including any unauthorized configuration changes, (2) router system log download covering the maximum retained window, (3) current routing table (`ip route show` or equivalent via Tenda CLI) and DNS forwarder settings to detect any attacker-planted DNS hijack entries, and (4) administrator account list from the router UI. These are volatile — they will be lost or altered the moment the device is powered down or replaced.

Step 4: Recovery — After isolation or replacement, verify that no unauthorized configuration changes persist: review routing tables, DNS forwarder settings, firewall rules, and administrator account lists. Confirm that management interface access is restricted to authorized management hosts only (NIST AC-3). Re-enable logging and alert on any future authentication attempts to management interfaces from unauthorized sources (NIST AU-2, AU-12, CIS 8.2). Monitor for lateral movement indicators in internal network traffic for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-3 (Access Enforcement), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: On the replacement router or upstream firewall, configure syslog forwarding to a central collector (rsyslog or syslog-ng on a Linux host) and write a cron-driven grep alert: `grep -E 'DENIED|REJECT' /var/log/firewall.log | grep -E '(80|443|8080)' | mail -s 'Router Mgmt Alert' soc@example.com`. For internal lateral movement monitoring post-remediation, deploy Wireshark or tcpdump on a span port with a capture filter for unexpected DNS query patterns (e.g., newly observed external resolvers, queries for dynamic DNS domains) that could indicate an attacker-planted DNS forwarder had already redirected internal clients before eradication.

Evidence: This step does not alter volatile live state on a newly replaced device, but before declaring recovery complete: verify the replacement device's firmware hash against the vendor's published checksum, confirm the router configuration matches the approved baseline (diff against the pre-incident backup captured in Step 3), and review DHCP logs on the replacement router for any clients that connected during the exposure window — those internal hosts should be triaged for signs of traffic redirection or credential harvesting that may have occurred while the backdoor was active.

Step 5: Post-Incident — This vulnerability exposes a control gap in network hardware inventory and lifecycle management. Audit all network edge devices for end-of-support or unpatched firmware status (CIS 1.1, CIS 2.2, CIS 7.1). Establish a process to track vendor advisories for all network infrastructure hardware and to replace unsupported devices on a defined schedule (CIS 7.2). Review whether router management interfaces were internet-facing in violation of documented policy (NIST AC-17, AC-22). Consider adding network device firmware integrity monitoring to the detection program (D3-SFA, D3-SICA).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AC-17 (Remote Access), NIST AC-22 (Publicly Accessible Content)

Compensating: Run Shodan queries (`shodan search 'tenda http.title:"Tenda"'`) or Censys searches against your organization's registered IP ranges to confirm no Tenda management interfaces remain internet-exposed. For ongoing firmware lifecycle tracking without a commercial tool, create a simple spreadsheet-based CMDB entry for every network device including model, current firmware version, vendor end-of-support date, and a CERT/CC VulnNote and NVD RSS feed subscription scoped to each vendor. Subscribe to CISA's Known Exploited Vulnerabilities (KEV) catalog RSS feed to catch future advisories for network hardware.

Evidence: No volatile evidence capture is required at the post-incident phase. Preserve for lessons-learned documentation: the original firewall log exports showing the exposure window (first external connection to router

management interface through to containment), the pre-eradication router configuration backup capturing any unauthorized changes, the timeline of when affected firmware versions were deployed versus when CVE-2026-11405 was disclosed, and any internal network traffic pcaps retained from the 30-day post-remediation monitoring window that may evidence lateral movement or DNS hijacking during the exposure period.

Detection Guidance

Query perimeter firewall logs for inbound connections to router management interface ports (commonly TCP 80, 443, 8080) originating from external IP ranges. Flag any successful HTTP 200 responses from the router management interface to external sources, as administrative access should not originate externally under normal policy. If the router produces access logs, review for authentication events that do not correspond to known administrator accounts or scheduled maintenance windows (NIST AU-6). Review router access logs for unexpected account creation or privilege escalation events, if the device supports such logging. No confirmed IOCs, exploit signatures, or specific event IDs are available from the provided source data. Active exploitation is reported by one non-authoritative source but has not been confirmed by CISA KEV or a direct CERT/CC advisory; detection posture should be elevated but exploitation should not be assumed confirmed.

Framework Mappings

MITRE-ATTACK

- **T1542.001** — System Firmware
- **T1133** — External Remote Services
- **T1040** — Network Sniffing
- **T1078** — Valid Accounts
- **T1556** — Modify Authentication Process
- **T1078.001** — Default Accounts
- **T1098** — Account Manipulation

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **SC-12** — Cryptographic Key Establishment and Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1542.001	System Firmware	Persistence
T1133	External Remote Services	Persistence
T1040	Network Sniffing	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access
T1078.001	Default Accounts	Defense-Evasion
T1098	Account Manipulation	Persistence

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/certcc-warns-of-hidden-admin-back...	T2
CVE-2026-11405 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-11405	T1
Active Exploitation Alert: Hidden Admin Backdoor (CVE-2026-11405 ...	https://www.rescana.com/post/active-exploitation-alert-hidden-admin...	T3
CVE-2026-56405 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-56405	T1
CVE-2026-11405 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-11405	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-11405	T1

Generated 2026-07-07 15:07 UTC by TJS Security Command Center