Smarttech
YOUR 24/7 SECURITY PARTNER

TP-Link Router Firmware Authentication Bypass Exposes Critical Security Weakness

Document ID	SMA-Informative Cyber Alert
Document status	ISSUED
Authors	Alex Ciuta < alexandru.ciuta@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	25th March 2026
Issue Date	25th March 2026

Informative Cyber Alerts are reports created by Smarttech247 designed to inform customers about medium and low severity vulnerabilities, IOCs from certain attacks/breaches, and other information that could help companies be aware and protect against any attack.
The content of this report should be regarded as simply informative as it usually addresses products that have an auto-update option available for patches. It will be the customer's decision if it is necessary to follow any recommendation or disregard them as they are not currently applicable in the environment.

Overview

TP-Link has released urgent firmware updates for several Archer NX routers to fix a critical authentication bypass flaw (CVE-2025-15517) that allows attackers to perform privileged actions, including uploading malicious firmware, without logging in. The company also patched a hardcoded cryptographic key issue and two command-injection bugs. TP-Link urges all users to update immediately, warning that unpatched devices remain at serious risk.

Technical Summary

TP-Link has patched several vulnerabilities in its Archer NX router series, including a critical-severity flaw that may allow attackers to bypass authentication and upload new firmware.

Tracked as CVE-2025-15517, this security flaw affects Archer NX200, NX210, NX500, and NX600 wireless routers and stems from a missing authentication weakness that attackers can exploit without privileges.

"A missing authentication check in the HTTP server to certain cgi endpoints allows unauthenticated access intended for authenticated users," TP-Link explained earlier this week when it released security updates that address the vulnerability.

Additionally, it addressed two command injection vulnerabilities (CVE-2025-15518 and CVE-2025-15519) that enable threat actors with admin privileges to execute arbitrary commands.

The company "strongly" recommended that customers download and install the latest firmware version to block potential attacks exploiting these flaws.

CVE	Score	Description
CVE-2025-15517	9.8	A missing authentication check in the HTTP server on TP-Link Archer NX200, NX210, NX500 and NX600 to certain cgi endpoints allows unauthenticated access intended for authenticated users. An attacker may perform privileged HTTP actions without authentication, including firmware upload and configuration operations.
CVE-2025-15518	7.2	Improper input handling in a wireless-control administrative CLI command on TP-Link Archer NX200, NX210, NX500 and NX600 allows crafted input to be executed as part of an operating system command. An authenticated attacker with administrative privileges may execute arbitrary commands on the operating system, impacting the confidentiality, integrity, and availability of the device.
CVE-2025-15519	7.2	Improper input handling in a modem-management administrative CLI command on TP-Link Archer NX200, NX210, NX500 and NX600 allows crafted input to be

		executed as part of an operating system command. An authenticated attacker with administrative privileges may execute arbitrary commands on the operating system, impacting the confidentiality, integrity, and availability of the device.

Affected Products

Affected Product	Affected Hardware Versions / Firmware Versions
Archer NX600	• v3.0: < 1.3.0 Build 260309 • v2.0: < 1.3.0 Build 260311 • v1.0: < 1.4.0 Build 260311
Archer NX500	• v2.0: < 1.5.0 Build 260309 • v1.0: < 1.3.0 Build 260311
Archer NX210	• v3.0: < 1.3.0 Build 260309 • v2.0 & v2.20: < 1.3.0 Build 260311
Archer NX200	• v3.0: < 1.3.0 Build 260309 • v2.20: < 1.3.0 Build 260311 • v2.0: < 1.3.0 Build 260311 • v1.0: < 1.8.0 Build 260311

Recommendations

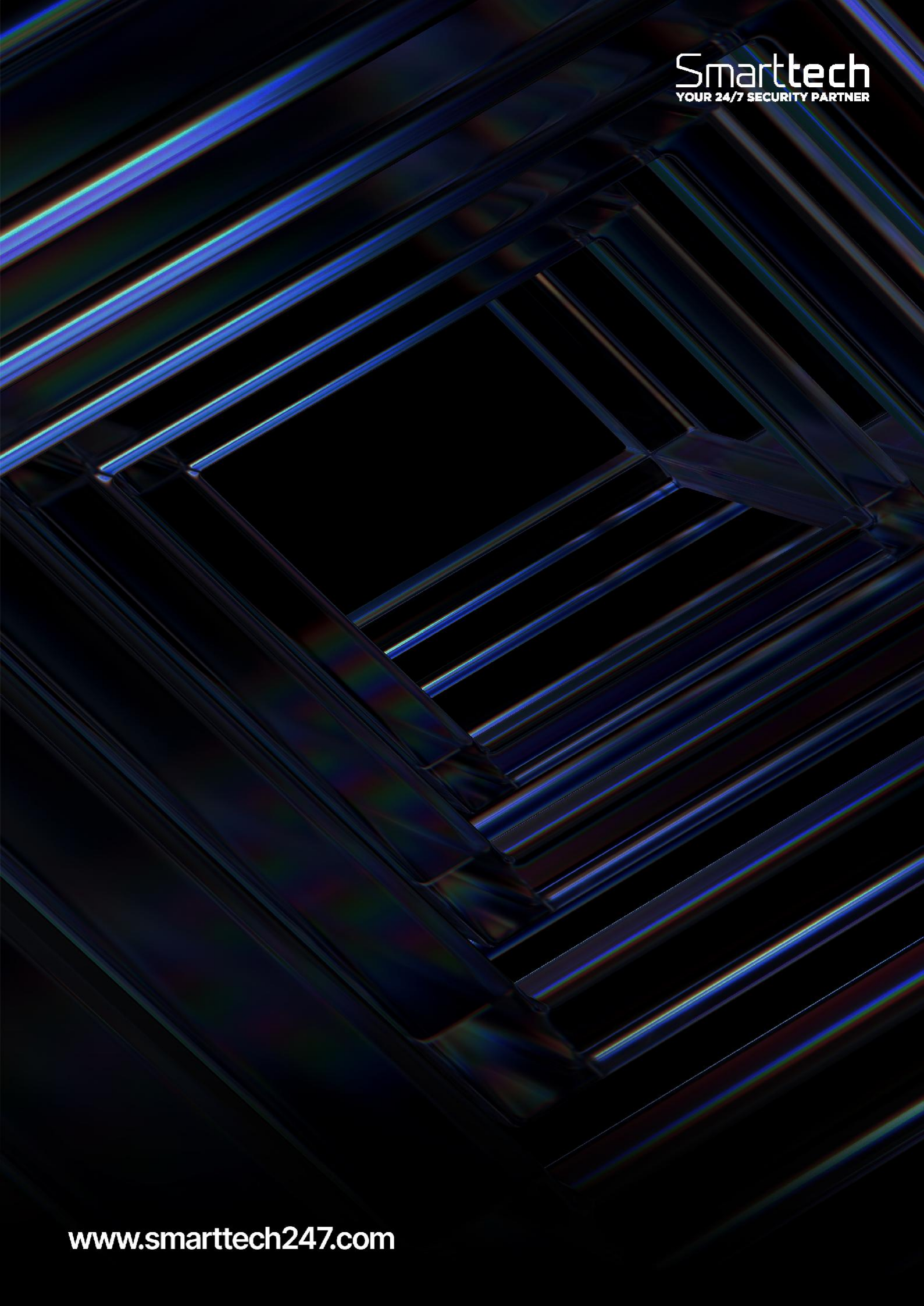
Smarttech247 team recommends the following actions to be taken:

- Install the latest TP-Link firmware update for your specific Archer NX model immediately to remediate CVE-2025-15517 and related vulnerabilities;
- Disable remote administration unless absolutely necessary, as remote access significantly increases exposure to unauthenticated exploitation;
- Ensure strong, unique administrative credentials remain in place—while this flaw bypasses authentication, robust passwords still reduce risk from other attack vectors;
- Back up and then reset device configurations after patching to eliminate any unauthorized changes made prior to the update;
- Regularly monitor router logs and network activity for signs of unauthorized configuration changes or unexpected firmware uploads;
- Segment critical devices from the main Wi-Fi network to limit lateral movement if a router compromise occurs;
- Enable automatic firmware update notifications to ensure future TP-Link security patches are applied promptly;
- Avoid using default or hardcoded cryptographic keys in any configuration backups, as previous flaws allowed attackers to decrypt and modify them;
- Reboot the router after applying patches to ensure all vulnerable services are fully replaced with updated components;
- Stay informed about newly disclosed TP-Link vulnerabilities, as multiple Archer-series flaws have been actively exploited in the past.

References

https://www.bleepingcomputer.com/news/security/tp-link-warns-users-to-patch-critical-router-auth-bypass-flaw/

https://www.tp-link.com/us/support/faq/5027/


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com