Statement on Hardcoded DES Decryption Keys in TP-Link Archer C50 V3/V4/V5 and C20 V5 (CVE-2025-6982)

Security Advisory

Last updated: April 22, 2026

Important Information:

These devices have reached end-of-life (EOL); therefore, please review the 'Recommendation(s)' section carefully.

Vulnerability Description:

Use of Hard-coded Credentials in TP-Link Archer C20 V5 and C50 V3(**<=** 180703)/V4(**<=** 250117)/V5(**<=** 200407), allows attackers to decrypt the config.xml file.

Impact:

This Hardcoded DES Decryption Keys may be used to decrypt the user config file.

CVSS v4.0 Score: 6.9 / Medium

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Affected Products/Versions and Fixes:

Affected Product Model	Related Vulnerabilities	Affected Version
TP-Link Archer C50 V3	CVE-2025-6982	**<=** 180703
TP-Link Archer C50 V4	CVE-2025-6982	**<=** 250117
TP-Link Archer C50 V5	CVE-2025-6982	**<=** 200407
TP-Link Archer C20 V5	CVE-2025-6982	**<** US_V5_260419 **<** EU_V5_260317

Recommendation(s):

EN: Download for Archer C20 | TP-Link

US: Download for Archer C20 | TP-Link

Disclaimer:

If you do not take the recommended action(s) stated above, this vulnerability concern will remain. TP-Link cannot bear any responsibility for the consequences that could have been avoided by following the recommended action(s) in this statement.

Related FAQs

Statement on cross-site scripting (XSS) vulnerability on TP-Link WR841N (CVE-2025-25427)

Statement on Tapo privilege escalation on shared devices using notifications (CVE-2025-4975)

Statement on the buffer overflow on TL-WR940N, TL-WR841N (CVE-2025-6151)

Statement on Clickjacking vulnerability on the management web application of TP-Link Archer C1200 (CVE-2025-6983)

Statement on authenticated and unauthenticated command injection on VIGI NVR1104H-4P V1 and VIGI NVR2016H-16MP V2 (CVE-2025-7723 and CVE-2025-7724)

Statement on the denial-of-service vulnerability due to the buffer overflow on TL-WR841N (CVE-2025-53711, CVE-2025-53712, CVE-2025-53713, CVE-2025-53714, CVE-2025-53715), TL-WR842ND (CVE-2025-53711) and TL-WR949N (CVE-2025-53711)

Looking For More

TP-Link Unveils World's 1st Batch WiFi 7 Tri-Band Network Adapter — Archer TBE550E

Archer AXE300 Unboxing

Is this faq useful?

Your feedback helps improve this site.

TP-Link Community

Still need help? Search for answers, ask questions, and get help from TP-Link experts and other users around the world.

Visit the Community >

Subscribe

Be The First To Get Exclusive Deals & News

Email Address | Subscribe

Let's Connect

before access or use.
References to "TP-Link" may include TP-Link Systems Inc., its subsidiaries, or business units within the TP-Link corporate structure, as applicable.
The materials provided, including but not limited to press releases, presentations, blog posts, and webcasts, are current as of the date of publication and may be superseded by subsequent updates.