

April Showers of Savings



Deals up to 50% off!



Security Advisory on Multiple Vulnerabilities on Archer AX53 (CVE-2026-30814, CVE-2026-30815, CVE-2026-30816, CVE-2026-30817, CVE-2026-30818)

Security Advisory

Updated 04-08-2026 17:57:35 PM

88

Multiple vulnerabilities were identified in TP-Link Archer AX53 v1.0 across the tmpserver, dnsmasq, and OpenVPN modules.

Description of Vulnerabilities and Impacts:

1. OS Command Injection Vulnerabilities

CVE-2026-30815: OpenVPN Module

An OS command injection vulnerability in the OpenVPN module allows an authenticated adjacent attacker to execute system commands when a specially crafted configuration file is processed due to insufficient input validation.

Successful exploitation may allow modification of configuration files, disclosure of sensitive information, or further compromise of device integrity.

CVE-2026-30818: dnsmasq Module

An OS command injection vulnerability in the dnsmasq module allows an authenticated adjacent attacker to execute arbitrary code when a specially crafted configuration file is processed due to insufficient input validation.

Successful exploitation may allow the attacker to modify device configuration, access sensitive information, or further compromise system integrity.

CVSS v4.0 Score: 8.5 / High

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

Welcome to Our Website! If you stay on our site, we and our third-party partners use cookies, pixels, and other tracking technologies to better understand how you use our services, and improve our services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).



Okay

Successful exploitation may cause a crash and could allow arbitrary code execution, enabling modification of device state, exposure of sensitive data, or further compromise of device integrity.

CVSS v4.0 Score: 7.3 / High

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

3. Arbitrary File Reading Vulnerabilities

CVE-2026-30816: OpenVPN Module

An external configuration control vulnerability in the OpenVPN module allows an authenticated adjacent attacker to read arbitrary files when a malicious configuration file is processed. Successful exploitation may allow unauthorized access to arbitrary files on the device, potentially exposing sensitive information.

CVE-2026-30817: dnsmasq Module

An external configuration control vulnerability in the OpenVPN module allows an authenticated adjacent attacker to read arbitrary files when a malicious configuration file is processed. Successful exploitation may allow unauthorized access to arbitrary files on the device, potentially exposing sensitive information.

Severity for CVE-2026-30816 and CVE-2026-30817

CVSS v4.0 Score: 6.8 / Medium

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

Affected Products/Versions and Fixes:

Product Model	Affected Version
Archer AX53 v1.0	< 1.7.1 Build 20260213

Recommendations:

We strongly recommend that users with affected devices take the following actions:

1. Download and update to the latest firmware version to fix the vulnerabilities:

EN: [Download for Archer AX53 | TP-Link](#)

MY: [Download for Archer AX53 | TP-Link Malaysia](#)

Note: AX53 v1 is not sold in the US.

Disclaimer:

If you do not take all recommended actions, these vulnerabilities may remain. TP-Link cannot bear any

Welcome to Our Website! If you stay on our site, we and our third-party partners use cookies, pixels, and other tracking technologies to better understand how you use our services, and improve our services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).



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

Let's Connect



About

- About Us
- Corporate Information
- Contact Us
- Sustainability
- Privacy Policy
- Your Privacy Choices
- Careers at TP-Link
- Accessibility
- Our Security Commitment

Press

- News
- Blog
- Security Advisory
- Security News
- Awards

Partners

- Partner Program
- Partner Deal Registration
- MAP Policy

Learning Center

- Technology Trends
- Training & Certification

Welcome to Our Website! If you stay on our site, we and our third-party partners use cookies, pixels, and other tracking technologies to better understand how you use our products and services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).





©2026 TP-Link Systems Inc. and its affiliated companies. All rights reserved.


 United States / English

TP-Link, Tapo, Kasa, Omada, VIGI, Aginet, HomeShield, and Tapo Care branded products are products of TP-Link Systems Inc. or its affiliates.

Note: Some services and materials may require you to accept additional terms and conditions 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.

Welcome to Our Website! If you stay on our site, we and our third-party partners use cookies, pixels, and other tracking technologies to better understand how you use our  provide and improve our services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).