tp-link

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

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

Your feedback helps improve this site.

Yes No

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