مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in TP-Link Archer Router

Tracking #:432315899

Date:28-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability exists in the TP-Link Archer C5400X gaming router.

TECHNICAL DETAILS:

A maximum-severity security flaw has been disclosed in the TP-Link Archer C5400X gaming router that could lead to remote code execution on susceptible devices by sending specially crafted requests.

The vulnerability, tracked as **CVE-2024-5035**, carries a CVSS score of 10.0. It impacts all versions of the router firmware including and prior to 1_1.1.6. It has been patched in version 1_1.1.7 released on May 24, 2024.

By successfully exploiting this flaw, remote unauthenticated attackers can gain arbitrary command execution on the device with elevated privileges.

Vulnerable version	<= 1_1.1.6
Fixed version	1_1.1.7

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the latest fixed version released by TP-link

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://www.tp-link.com/ae/support/download/archer-c5400x/