



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in Asus Router Models

Tracking #:432315972

Date:21-06-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Asus released security updates to address a critical security flaw impacting its routers that could be exploited by malicious actors to bypass authentication.

TECHNICAL DETAILS:

Asus released security updates for its routers that addresses a vulnerability in some ASUS router models, allowing remote attackers to log into the device without authentication.

CVE ID: CVE-2024-3080- Improper Authentication

CVSS 3.x Severity and Metrics: Score: 9.8 Critical

Affected Products:

- ZenWiFi XT8 version 3.0.0.4.388_24609 and earlier
- ZenWiFi XT8 version V2 3.0.0.4.388_24609 and earlier
- RT-AX88U version 3.0.0.4.388_24198 and earlier
- RT-AX58U version 3.0.0.4.388_23925 and earlier
- RT-AX57 version 3.0.0.4.386_52294 and earlier
- RT-AC86U version 3.0.0.4.386_51915 and earlier
- RT-AC68U version 3.0.0.4.386_51668 and earlier

Fixed Versions:

- ZenWiFi XT8 to version 3.0.0.4.388_24621 or later
- ZenWiFi XT8 V2 to version 3.0.0.4.388_24621 or later
- RT-AX88U to version 3.0.0.4.388_24209 or later
- RT-AX58U to version 3.0.0.4.388_24762 or later
- RT-AX57 to version 3.0.0.4.386_52303 or later
- RT-AC86U to version 3.0.0.4.386_51925 or later
- RT-AC68U to version 3.0.0.4.386_51685 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates released by Asus.

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:

- <https://www.twcert.org.tw/tw/cp-132-7859-0e104-1.html>