CVE-2025-2492: IMPROPER AUTHENTICATION IN ASUS ROUTERS WITH AICLOUD

Vairav CVE Report

Date: April 21, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

ASUS has released firmware updates addressing **CVE-2025-2492**, a critical remote code execution vulnerability affecting several ASUS router firmware series with **AiCloud enabled**. This flaw, rated **CVSSv4 9.2 (Critical)**, allows unauthenticated remote attackers to execute unauthorized functions and compromise the network. Users are strongly advised to update their router firmware immediately and disable internet-facing services if updates are not feasible.

VULNERABILITY DETAILS

CVE-2025-2492: Improper Authentication in ASUS Routers with AiCloud

Description: The vulnerability is caused by improper authentication control in the ASUS AiCloud component. A crafted request can bypass authentication and trigger the execution of unauthorized router functions.

Impact: Remote attackers can compromise router operations, access connected devices, and potentially exfiltrate sensitive data**.**

CVSS Score: 9.2 (Critical)

Exploitation: An attacker can craft a malicious request to trigger unauthorized actions without needing valid credentials.

AFFECTED PRODUCTS/VERSIONS

ASUS Router firmware series: 3.0.0.4_382, 3.0.0.4_386, 3.0.0.4_388, 3.0.0.6_102

- Fixed in firmware updates released after February 2025.

RECOMMENDATIONS

- **Update Firmware:** Immediately install the latest firmware from the ASUS Support Page.
- **Strengthen Passwords:** Use passwords with at least 10 characters, including uppercase letters, numbers, and symbols.
- **Disable Risky Services:** If unable to update promptly or use an unsupported router, disable the following: AiCloud, Remote access from WAN, Port forwarding, DDNS, VPN server, DMZ, FTP, and port triggering.

- **Monitor System Logs and Settings:** Regularly audit router logs and verify security settings to ensure no unauthorized access.

REFERENCES

https://securityonline.info/cve-2025-2492-critical-asus-router-vulnerability-requires-immediate-firmware-update/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com