مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerabilities in ASUS Routers

Tracking #:432316698
Date:03-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed high-severity vulnerabilities in Asus routers that could potentially allow attackers to execute malicious commands on the affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-12912** and **CVE-2024-13062**
- CVSS score 7.2 High
- Security vulnerabilities exists in Asus routers. These vulnerabilities could allow attackers to execute arbitrary commands on vulnerable devices.
- The vulnerabilities stem from injection and execution flaws in certain ASUS router firmware series, specifically within the **AiCloud service**. Exploiting these flaws requires authentication.
- Successful exploitation of this vulnerabilities could lead to unauthorized command execution, compromising the device and the broader network.

Affected Models and Firmware:

- While the specific router models affected are not explicitly available, ASUS is urging users of various router firmware series to update immediately. The vulnerable firmware versions include:
  - 3.0.0.4_386 series
  - 3.0.0.4_388 series
  - 3.0.0.6_102 series

RECOMMENDATIONS:

- **Firmware Updates**: Update routers to the latest firmware version.
- **Strong Password Practices**:
  - Use different passwords for the wireless network and router administration page
  - Implement passwords with at least 10 characters, including a mix of capital letters, numbers, and symbols
- **AiCloud Protection**: Enable password protection within the AiCloud service to add an extra layer of security.
- **Disable External Services**: To minimize potential attack vectors, disable services accessible from the internet, including:
  - Remote access
  - Port forwarding
  - DDNS
  - VPN server
  - DMZ
  - FTP

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.asus.com/content/asus-product-security-advisory/