مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in ASUS DSL Routers

Tracking #:432318029

Date:18-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical authentication bypass vulnerability ASUS DSL Series Routers. This flaw allows remote attackers to gain access to affected devices without valid credentials.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-59367**
- **CVSSv4 Score:** 9.3 (Critical)
- A critical authentication bypass exists in certain ASUS DSL routers that allows remote attackers to access the device without valid credentials. The flaw can be exploited over the internet on devices with exposed management interfaces.
- Successful exploitation of this vulnerability can allow attackers to gain full administrative control over the affected router, modify settings, intercept or redirect network traffic, install malware, and compromise connected devices.

Affected Models and Fixed Firmware Versions:

- ASUS DSL Series routers: DSL-AC51, DSL-N16, and DSL-AC750.

Fixed Versions:

- Firmware version 1.1.2.3_1010 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions 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.cve.org/CVERecord?id=CVE-2025-59367