مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Asus Router
Tracking #:432318077
Date:27-11-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that ASUS has released security updates to address multiple vulnerabilities in its Asus Router.

TECHNICAL DETAILS:

Security researchers have identified multiple vulnerabilities affecting ASUS router firmware across the 3.0.0.4_386, 3.0.0.4_388, and 3.0.0.6_102 series. ASUS has released updated firmware (October 2025 release) that mitigates the disclosed vulnerabilities. Users of End-of-Life (EOL) router models, which will not receive new firmware updates, must apply configuration-based mitigations to reduce exposure. These vulnerabilities range from Medium to Critical severity, with potential impacts including unauthorized access, high-impact availability compromise, and remote exploitation depending on the specific CVE.ASUS strongly urges all users to update their router firmware immediately to the latest available version.

1. CVE-2025-59365
   - CVSS 4.0 Score: 6.9 (Medium)

2. CVE-2025-59366
   - CVSS 4.0 Score: 9.2 (Critical)

3. CVE-2025-59368
   - CVSS 4.0 Score: 6.0 (Medium)

4. CVE-2025-59369
   - CVSS 4.0 Score: 5.9 (Medium)

5. CVE-2025-59370
   - CVSS 4.0 Score: 7.5 (High)

6. CVE-2025-59371
   - CVSS 4.0 Score: 7.5 (High)

7. CVE-2025-59372
   - CVSS 4.0 Score: 6.9 (Medium)

8. CVE-2025-12003
   - CVSS 4.0 Score: 8.2 (High)

Affected Products:
   - 3.0.0.4_386 series
   - 3.0.0.4_388 series
   - 3.0.0.6_102 series

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update firmware immediately for the affected routers.

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/security-advisory/