مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in ASUS DriverHub

Tracking #:432317251

Date:12-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in the ASUS DriverHub software, a tool designed to simplify driver updates for ASUS motherboards. These vulnerabilities could allow malicious actors to compromise affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-3462 (CVSSv4 Score: 8.4** High**) – Insufficient Validation of HTTP Requests**
  - This flaw allows attackers to **spoof internal communications** and interact with features typically reserved for trusted sources.
- **CVE-2025-3463 (CVSSv4 Score: 9.4** Critical**) – Remote System Manipulation via Crafted Requests**
  - This vulnerability enables **untrusted sources to manipulate system behavior**, potentially compromising motherboard security.

Affected Versions:

- ASUS DriverHub versions prior to 1.0.6.0

Fixed Versions:

- ASUS DriverHub versions 1.0.6.0 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.asus.com/content/asus-product-security-advisory/