مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in ASUS Servers

Tracking #:432317115

Date:25-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability (CVE-2024-54085) has been discovered in AMI's MegaRAC BMC firmware, used extensively across servers from multiple OEMs, including ASUS.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2024-54085) has been discovered in AMI's MegaRAC BMC firmware, used extensively across servers from multiple OEMs, including ASUS. This flaw enables local or remote attackers to fully control affected servers by exploiting the Redfish management interface, a standard for out-of-band server management.

Vulnerability Details:

- Vulnerability ID: **CVE-2024-54085**
- CVSS v4 Score: 10.0 (Critical)
- Affected Vendors: ASUS, Lenovo,HPE, ASRock, and others
- HPE and Lenovo have already released security updates for their products that integrate AMI's Fix.
- The vulnerability, if successfully exploited, allows attackers to:
  - Install persistent malware or ransomware
  - Conduct firmware-level tampering
  - Brick servers by triggering over-voltage conditions
  - Create indefinite reboot loops
  - Disable hardware components irreversibly

Affected ASUS Models and Patched Firmware Versions:

- PRO WS W790E-SAGE SE: v1.1.57
- PRO WS W680M-ACE SE: v1.1.21
- PRO WS WRX90E-SAGE SE: v2.1.28
- Pro WS WRX80E-SAGE SE WIFI: v1.34.0

RECOMMENDATIONS:

- **Update Firmware:** Upgrade to the latest BMC firmware versions for affected ASUS motherboards.

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://go.ami.com/hubfs/Security%20Advisories/2025/AMI-SA-2025003.pdf