مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in ABB ASPECT System

Tracking #:432316609

Date:10-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed ABB has issued an urgent cyber security advisory for its ASPECT system, a building energy management platform, detailing critical vulnerabilities that could allow attackers to remotely control the system and potentially execute malicious code.

TECHNICAL DETAILS:

ABB has issued an urgent cyber security advisory for its ASPECT system, a building energy management platform, detailing critical vulnerabilities that could allow attackers to remotely control the system and potentially execute malicious code. The vulnerabilities, ranging from remote code execution (RCE) to denial-of-service (DoS) attacks, affect multiple versions of ASPECT and have been assigned CVSS v3.1 base scores as high as 10.0, indicating their severe risk. Immediate action is required to mitigate potential threats to building systems that could result in unauthorized access, system compromise, and disruption of operations.

Vulnerabilities Overview:

- **CVE-2024-6298 (CVSS 10.0)** – Remote Code Execution (RCE):
  - Improper input validation in ASPECT allows attackers to execute arbitrary code remotely, enabling them to take full control of the affected system and potentially insert malicious code.
- **CVE-2024-6515 (CVSS 9.6)** – Clear Text Passwords:
  - ASPECT systems may handle passwords in clear text or Base64 encoding, exposing credentials and increasing the risk of unauthorized access and credential theft.
- **CVE-2024-51551 (CVSS 10.0)** – Default Credentials:
  - Devices using publicly available default credentials are highly vulnerable to unauthorized access. Immediate credential changes are necessary to secure the system.
- **CVE-2024-51549 (CVSS 10.0)** – Absolute Path Traversal:
  - An attacker can exploit this flaw to gain access to unintended resources and modify critical files, increasing the risk of system compromise.

Fixed Versions:

- ASPECT systems version 3.08.03 or later

RECOMMENDATIONS:

- Immediately disconnect any ASPECT systems that are directly connected to the internet or are exposed due to insecure network configurations.
- Upgrade all ASPECT systems to fixed version or later.
- Ensure that all ASPECT systems are placed behind secure firewalls and use Virtual Private Networks (VPNs) for remote access.
- Immediately change default credentials on all ASPECT devices. Use strong, unique passwords to prevent unauthorized access from exploiting default credentials.

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://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch