مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in ABB Ability Edgenius

Tracking #:432318058

Date:24-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical authentication bypass vulnerability in the ABB Ability Edgenius Management Portal. This flaw enables unauthenticated attackers to gain direct access to privileged functions within affected systems.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-10571**
- CVSS v3.1 Base Score: 9.6 Critical
- The vulnerability stems from improper authentication handling, allowing attackers to interact with protected functions without providing valid credentials. A specially crafted message sent to an Edgenius system node can trigger the flaw.
- Successful exploitation allows an unauthenticated attacker to:
  - Install or uninstall applications
  - Execute arbitrary code
  - Modify configurations of deployed applications
  - Gain full administrative control over the edge environment

Affected Versions:

- ABB Ability Edgenius **3.2.0.0** and **3.2.1.1**

Fixed Versions:

- ABB Ability Edgenius **3.2.2.0 or later**

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by ABB.

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=7PAA022088&LanguageCode=en&DocumentPartId=&Action=Launch