مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in ABB FLXeon Controllers

Tracking #:432316806

Date:30-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed ABB has identified and addressed multiple critical vulnerabilities in its FLXeon controllers, which could allow attackers to execute remote code, bypass authentication, and access sensitive information

TECHNICAL DETAILS:

ABB has identified and addressed multiple critical vulnerabilities in its FLXeon controllers, which could allow attackers to execute remote code, bypass authentication, and access sensitive information.

Vulnerability Details

1. **CVE-2024-48841 (CVSS 10.0): Remote Code Execution (RCE)**
   - **Description**: This critical vulnerability allows attackers with network access to execute arbitrary code with elevated privileges. The issue arises from improper control of filenames in PHP program statements (CWE-98).
   - **Impact**: Successful exploitation could lead to a complete system compromise, enabling attackers to take full control of the affected device.
   - **Affected Versions**: FLXeon firmware versions 9.3.4 and older.
   - **Mitigation**: Upgrade to firmware version 9.3.5 or later.

2. **CVE-2024-48849 (CVSS 9.4): Authentication and Authorization Issues**
   - **Description**: Inadequate session management allows attackers to bypass authentication mechanisms and send unauthorized HTTPS requests.
   - **Impact**: Attackers could gain access to restricted resources, manipulate system operations, or disrupt normal functionality.
   - **Affected Versions**: FLXeon firmware versions 9.3.4 and older.
   - **Mitigation**: Upgrade to firmware version 9.3.5 or later and enforce strong authentication practices.

3. **CVE-2024-48852 (CVSS 9.4): Information Disclosure**
   - **Description**: Sensitive information may be improperly disclosed through HTTPS access due to insecure logging practices (CWE-532).
   - **Impact**: Disclosure of critical data could facilitate further exploitation or compromise of the system.
   - **Affected Versions**: FLXeon firmware versions 9.3.4 and older.
   - **Mitigation**: Upgrade to firmware version 9.3.5 or later and review logging configurations to ensure sensitive information is not exposed.

RECOMMENDATIONS:

- Update FLXeon controllers to fixed firmware version.
- Ensure FLXeon devices are not directly exposed to the internet.
- Place controllers behind firewalls and implement strict access control lists (ACLs) to limit access to authorized users and systems only.

- Regularly review system logs for unusual activity, such as unauthorized access attempts or unexpected changes to system configurations.
- Ensure sensitive information is not logged in plaintext or exposed through insecure channels.
- Enforce multi-factor authentication (MFA) for all users accessing FLXeon controllers.

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=9AKK108470A5684&LanguageCode=en&DocumentPartId=PDF&Action=Launch