مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in General Industrial Controls Lynx+ Gateway

Tracking #:432318028

Date:18-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple critical vulnerabilities in the General Industrial Controls (GIC) Lynx+ Gateway devices.

TECHNICAL DETAILS:

Multiple critical vulnerabilities identified in the General Industrial Controls (GIC) Lynx+ Gateway, versions R08, V03, V05, and V18. These flaws include weak authentication controls, missing authentication in critical functions, and cleartext transmission of sensitive information.

Successful exploitation could allow a remote, unauthenticated attacker to obtain sensitive device data, compromise system credentials, gain unauthorized access, or reset the device, potentially leading to operational disruption in industrial environments.

These vulnerabilities pose a high risk to organizations in the Critical Manufacturing sector and other environments deploying Lynx+ Gateway devices.

Vulnerability Details:

1. CVE-2025-55034 – Weak Password Requirements (CWE-521)
   - CVSS v3: 8.2 (High)
     CVSS v4: 8.8 (High)
   - Description: The device enforces weak password complexity, making it susceptible to brute-force attacks. An unauthenticated attacker could leverage this weakness to gain unauthorized access to the device's interface.

2. CVE-2025-58083 – Missing Authentication for Critical Function (CWE-306)
   - CVSS v3: 10.0 (Critical)
     CVSS v4: 9.2 (Critical)
   - Description: The embedded web server lacks authentication for a critical device-reset function. A remote attacker can reset the device without credentials, leading to disruption of industrial processes.

3. CVE-2025-59780 – Missing Authentication for Sensitive Information (CWE-306)
   - CVSS v3: 7.5 (High)
     CVSS v4: 8.7 (High)
   - Description: The web interface lacks authentication for sensitive GET requests, allowing an attacker to retrieve device configuration details or sensitive operational information.

4. CVE-2025-62765 – Cleartext Transmission of Sensitive Information (CWE-319)
   - CVSS v3: 7.5 (High)
     CVSS v4: 8.7 (High)
   - Description: The device transmits sensitive data—including credentials—in cleartext. A network-accessible attacker could intercept traffic to obtain usernames, passwords, or configuration data.

Affected Products:

- Lynx+ Gateway R08
- Lynx+ Gateway V03
- Lynx+ Gateway V05
- Lynx+ Gateway V18

RECOMMENDATIONS:

- Contact General Industrial Controls (GIC) for official patch status.
- Segment Lynx+ Gateway devices from business networks using industrial DMZs.
- Restrict access to the device using firewall rules and ACLs.
- Disable all unnecessary network services and ports.
- Enforce VPN-based remote access with MFA.

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.cisa.gov/news-events/ics-advisories/icsa-25-317-08