مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Unauthenticated Access Vulnerability in Synectix LAN 232 TRIO

Tracking #:432318357

Date:05-02-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been identified in the Synectix LAN 232 TRIO serial-to-Ethernet adapter that allows unauthenticated remote attackers to fully compromise affected devices.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in the Synectix LAN 232 TRIO serial-to-Ethernet adapter that allows unauthenticated remote attackers to fully compromise affected devices.
Tracked as CVE-2026-1633, this flaw exposes the device's web management interface without requiring authentication. An attacker with network access can directly modify critical configuration settings or perform a factory reset, potentially causing operational disruption or complete loss of connectivity to connected industrial equipment.

The vulnerability carries a CVSS v3.1 base score of 10.0 (Critical), indicating maximum severity and ease of exploitation.

Compounding the risk, Synectix is no longer operational, meaning no firmware patches or vendor mitigations will ever be released. All versions of the product are permanently vulnerable.
Organizations using this hardware should treat it as end-of-life and unpatchable and take immediate action to remove or isolate affected devices.

Vulnerability Overview

- **CVE ID:** CVE-2026-1633
- **Weakness Classification:** CWE-306 – Missing Authentication for Critical Function
- **CVSS v3.1 Base Score:** 10.0 (Critical)
- Web management interface is exposed without any authentication
- No username or password required to access administrative functions
- Any user with network access can:
  - Modify critical device settings
  - Factory reset the device
  - Disrupt serial-to-Ethernet communications
  - Potentially impact connected industrial systems
- No exploitation complexity:
  - No credentials required
  - No user interaction required
  - No special tools needed

Attackers only need to browse to the device IP address to gain full administrative control.

Affected Product

- **Vendor:** Synectix
- **Product:** LAN 232 TRIO (3-Port Serial to Ethernet Adapter)
- **Versions:** All versions

RECOMMENDATIONS:

1. **Identify all Synectix LAN 232 TRIO devices**
   - Perform asset discovery across OT and IT networks.
2. **Physically remove and replace affected hardware**
   - This is the only permanent remediation.
3. **Replace with supported alternatives**
   - Use actively maintained serial-to-Ethernet adapters from reputable vendors.

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.cve.org/CVERecord?id=CVE-2026-1633