مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Delta Electronics DIALink

Tracking #:432317730

Date:19-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Delta Electronics DIALink, a widely used industrial networking tool. If exploited, the flaws could allow attackers to bypass authentication and gain unauthorized access to critical systems.

TECHNICAL DETAILS:

Two serious vulnerabilities have been identified in Delta Electronics DIALink, a widely used industrial networking tool. Successful exploitation could allow an attacker to bypass authentication and gain unauthorized access to critical systems. Both flaws arise from improper directory path handling and pose a significant risk to industrial environments if left unpatched.

Vulnerability Details

- CVE-2025-58320
  - Type: Path Traversal (Improper limitation of a pathname to a restricted directory)
  - CVSS v3.1 Score: 7.3 (High)
  - Impact: Exploitation may allow manipulation of file system access and partial bypass of security controls.
- CVE-2025-58321
  - Type: Path Traversal (Improper limitation of a pathname to a restricted directory)
  - CVSS v3.1 Score: 10.0 (Critical)
  - Impact: Exploitation could lead to complete authentication bypass, granting an attacker unrestricted access to the underlying system.

Impact

Exploitation of these vulnerabilities could enable attackers to:

- Bypass authentication and gain unauthorized system access
- Disrupt operational processes in industrial environments
- Steal sensitive information
- Use compromised systems as a pivot point into broader enterprise networks

Affected Products

- Delta Electronics DIALink V1.6.0.0 and prior

Fixed Versions

- Delta Electronics DIALink V1.8.0.0 and later

RECOMMENDATIONS:

- Upgrade to DIALink V1.8.0.0 or later.
- Apply the following security best practices:
  - Do not expose control systems directly to the Internet.
  - Place systems behind firewalls and isolate from business networks.
  - Use secure remote access methods, such as VPNs, when required.

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-25-259-07