ADVANTECH Enabling an Intelligent Planet

No. 1, Alley 20, Lane 26, Rueiguang Road,
Neihu District, Taipei 11491, Taiwan, R.O.C.
Tel: 886-2-2792-7818
Fax: 886-2-2218-3650

SECURITY ADVISORY

Vulnerabilities Identified in ECU-1251D

This document summarizes the vulnerabilities identified in the ECU-1251D product, the associated CVEs, and the remediation actions completed by Advantech.

Vulnerability Type, Impact and Solution

Item	CVE ID	CVSS score	Impact	Solution
1	CVE-2026-6889	6.9	The Advantech ECU-1251D is vulnerable to a denial of service (DoS) due to improper handling of malformed DNP signals targeting Digital Output addresses. An attacker can send crafted DNP messages at timed intervals to force the device into an indefinite restart loop triggered by its internal daemon. During this condition, SCADA connections are disrupted while other interfaces remain accessible, preventing operator visibility and control until a manual restart is performed. An attacker may continue interacting with the device via these interfaces and modify system parameters. When combined with CVE-2026-6890 (Use of Default Credentials), this issue may enable authenticated changes while the operator's interface remains unavailable.	After internal analysis, we confirmed that this issue is not caused by periodic requests from TelWin. Instead, the root cause lies in the DNP3Daemon application, which receives DNP3 requests sent by TelWin. When processing DO signals, this daemon invokes an incorrect system file, resulting in program termination. DNP3Server selects either libboardio.so or the direct dc_tag_write method to operate digital outputs (DO) based on tag_type. For device models whose DO channels do not support PWM features, selecting a boardIO tag will trigger a call to the non-existent libboardio.so file and cause execution failure. The following adjustments have been implemented: • For device models with PWM-capable DO channels: When BO tags are linked on the DNP3Server configuration page, tag_type="boardIO" will be written to the configuration file if a boardIO tag is selected; if a non-boardIO tag (e.g., user tag) is chosen, tag_type="normalIO" will be applied instead. • For device models without PWM support on DO channels: All selected BO tags will uniformly use tag_type="normalIO".
2	CVE-2026-6890	7.1	The Advantech ECU-1251D uses default credentials, providing an account with username root and no password as described in the device documentation.	A prompt indicating weak password security appears when logging in as root via SSH, recommending a password change.

No. 1, Alley 20, Lane 26, Rueiguang Road,
Neihu District, Taipei 11491, Taiwan, R.O.C.
Tel: 886-2-2792-7818
Fax: 886-2-2218-3650

			While intended for initial setup, the documentation does not clearly indicate that these credentials should be changed, which may lead to deployments retaining the default configuration. This account can be used to access the device via SSH. As a result, an attacker may leverage these default credentials to gain unauthorized access to the device and interact with its configuration and parameters. CWE-1392	

Credits

Advantech would like to thank the following researchers for responsibly disclosing the vulnerabilities:

- Vulnerability disclosure is a result of GAZ-SYSTEM OT ARENA training with cooperation with WOT and CSIRT NASK

Additionally, Advantech would like to thank CSA for their collaboration on the coordinated disclosure process.

Affected Products

We strongly recommend all users update their devices to this latest firmware version (EdgeLink2.8.5.0) as soon as possible. The update is available for download on our official website.

Model Name	Download Page
ECU-1251D	ECU-1251D EdgeLink Image - 研华技术支持

Revision History

Version	Description	Release Date
1.0	First Advisory published	October,27,2026