# Product Advisory

| | | | |
|---|---|---|---|
| ***Product Family:*** | DirectLOGIC | ***Number:*** | PA-DL-003 |
| ***Part Numbers:*** | See Affected Part Numbers table below | ***Date Issued:*** | 09/14/2022 |
| ***Subject***: | DirectLOGIC with Serial communication security vulnerability | ***Revision:*** | Original |

## Purpose

This Product Advisory is related to Cyber Security and is intended to notify customers of a software or firmware vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or offer workarounds that can minimize the potential risk as much as possible.

## Affected Products

Hardware: DirectLogic DL105 products with the following part numbers:

| Part Number | Products and Affected Versions |
|---|---|
| F1-130AA | All |
| F1-130AD | All |
| F1-130DA | All |
| F1-130DD | All |
| F1-130DD-D | All |
| F1-130DR-D | All |
| F1-130AR | All |
| F1-130DR | All |

## Summary

AutomationDirect is aware of a vulnerability in the products listed above.

Vulnerability Type: Serial Exploit to Retrieve PLC Password

If an attacker has access to the PLC serial ports, they could send a specifically crafted serial message to the CPU serial port that would cause it to reply with the PLC password in clear text. This could allow the attacker to use the password to access and make unauthorized changes to the project or the interrupt the process

## Vulnerability Classification

AutomationDirect rates the severity level of the Vulnerabilities with a CVSS score of High.

## Remediation

The following actions are recommended:

| | |
|---|---|
| **All DL105 CPUs (F1-130xx)** | **This product is obsolete and cannot be upgraded. Recommend to upgrade to newer PLC (PLC families listed in Mitigation section).** |

## Mitigations

While Automation Networks and Systems have built-in password protection schemes, this is only one very small step in securing your systems. Automation Control System Networks need to incorporate data protection and security measures that are at least as robust as a typical business computer system. We recommend that users of PLCs, HMI products and SCADA systems perform your own network security analysis to determine the proper level of security required for you application.

AutomationDirect has identified the specific mitigation actions listed below:

- Secure physical access
- Isolate and air gap networks when possible.
- Consider some of the AutomationDirect newer PLC families (CLICK, Do-more/BRX and Productivity Series).

Please follow the security considerations in the following document:
https://support.automationdirect.com/docs/securityconsiderations.pdf

## Product Description

The DirectLogic product line is the original PLC family provided by AutomationDirect. This product was started in the 1980’s.

## Technical Assistance

If you have any questions regarding this Product Advisory, please contact Technical Support at 770-844-4200 or 800-633-0405 for further assistance.