Product Advisory

Product Family:	DirectLOGIC	***Number:***	PA-DL-001
Part Numbers:	See Affected Part Numbers table below	***Date Issued:***	08/25/2022
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 CPU products with the following part numbers:

Part Number	Products and Affected Versions
D0-05DD	Firmware version prior to V5.41
D0-05DR	Firmware version prior to V5.41
D0-05DA	Firmware version prior to V5.41
D0-05AR	Firmware version prior to V5.41
D0-05AA	Firmware version prior to V5.41
D0-05AD	Firmware version prior to V5.41
D0-05DD-D	Firmware version prior to V5.41
D0-05DR-D	Firmware version prior to V5.41
D2-230	All
D2-240	All
D2-250	All
D2-250-1	Firmware version prior to V4.91
D2-260	Firmware version prior to V2.71
D2-262	Firmware version prior to V1.06
D3-350	All
D4-430	All
D4-440	All
D4-450	All
D4-454	Firmware version prior to V1.04

Note: All D0-06xx PLCs are affected as well. Details for these devices are addressed in a previous Product Advisory (PA-D06-015) and can be found here: https://cdn.automationdirect.com/static/firmware/product_advisory/PA-D06-014_015.pdf

Product Advisory

Summary

AutomationDirect is aware of vulnerabilities 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 DL05 CPUs (D0-05xx)	**Upgrade firmware to version 5.41 or later**
D2-230/240/250	**This product is obsolete and cannot be upgraded. Recommend to upgrade to newer PLC (D2-262 or newer PLC families listed in Mitigation section).**
D2-250-1	**Upgrade firmware to version 4.91 or later**
D2-260	**Upgrade firmware to version 2.71 or later**
D2-262	**Upgrade firmware to version 1.06 or later**
D3-350	**This product is obsolete and cannot be upgraded. Recommend to upgrade to newer PLC (PLC families listed in Mitigation section).**
D4-430/440/450	**This product is obsolete and cannot be upgraded. Recommend to upgrade to newer PLC (D4-454 or PLC families listed in Mitigation section).**
D4-454	**Upgrade firmware to version 1.04 or later**

All DirectLogic PLC firmware can be found here under **PRODUCT FIRMWARE**:
https://www.automationdirect.com/support/software-downloads?itemcode=DirectSOFT%206

This version of firmware will no longer respond with the password when requested with the specially crafted message.

Additional brute force mitigation for password access has also been added. Three incorrect password entries will result in a 3 hour lock out of password entry. Power cycle will allow subsequent password attempts.

Product Advisory

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.

Product Advisory

Product Family:	DirectLOGIC	***Number:***	PA-DL-002
Part Numbers:	See Affected Part Numbers table below	***Date Issued:***	08/25/2022
Subject:	DirectLOGIC with Ethernet 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 products with the following part numbers:

Part Number	Products and Affected Versions
H0-ECOM & H0-ECOM100 when installed in the following D0-05 series CPUs:	All
D0-05DD	Firmware version prior to V5.41
D0-05DR	Firmware version prior to V5.41
D0-05DA	Firmware version prior to V5.41
D0-05AR	Firmware version prior to V5.41
D0-05AA	Firmware version prior to V5.41
D0-05AD	Firmware version prior to V5.41
D0-05DD-D	Firmware version prior to V5.41
D0-05DR-D	Firmware version prior to V5.41
H2-ECOM & H2-ECOM100 when installed in the following	All
D2-240	All
D2-250	All
D2-250-1	Firmware version prior to V4.91
D2-260	Firmware version prior to V2.71
D2-262	Firmware version prior to V1.06
H2-ECOM & H4-ECOM100 when installed in the following	All
D4-430	All
D4-440	All
D4-450	All
D4-454	Firmware version prior to V1.04

Note: All D0-06xx PLCs with H0-ECOM and H0-ECOM100 modules installed are affected as well. Details for these devices are addressed in a previous Product Advisory (PA-D06-014) and can be found here: https://cdn.automationdirect.com/static/firmware/product_advisory/PA-D06-014_015.pdf

Product Advisory

Summary

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

Vulnerability Type: Ethernet Exploit to Retrieve PLC Password

If an attacker has access to the PLC, a specially crafted packet can be sent to the PLC via Ethernet to access the password. This could allow the attacker to use the password to retrieve and/or make unauthorized changes to the project or interrupt the process.

Vulnerability Classification

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

Remediation

No Ethernet firmware changes are required. Only PLC CPU firmware should be upgraded (for the models this is applicable to). The following actions are recommended:

All DL05 CPUs (D0-05xx)	**Upgrade firmware to version 5.41 or later**
D2-240/250	**This product is obsolete and cannot be upgraded. Recommend to upgrade to newer PLC (D2-262 or newer PLC families listed in Mitigation section).**
D2-250-1	**Upgrade firmware to version 4.91 or later**
D2-260	**Upgrade firmware to version 2.71 or later**
D2-262	**Upgrade firmware to version 1.06 or later**
D4-430/440/450	**This product is obsolete and cannot be upgraded. Recommend to upgrade to newer PLC (D4-454 or PLC families listed in Mitigation section).**
D4-454	**Upgrade firmware to version 1.04 or later**

All DirectLogic PLC firmware can be found here under **PRODUCT FIRMWARE**:
https://www.automationdirect.com/support/software-downloads?itemcode=DirectSOFT%206

This version of firmware will no longer respond with the password when requested with the specially crafted message.

Additional brute force mitigation for password access has also been added. Three incorrect password entries will result in a 3 hour lock out of password entry. Power cycle will allow subsequent password attempts.

Product Advisory

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.