Product Advisory

Product Family:	DirectLOGIC w/ EtherNet Communication Modules	***Number:***	PA-D06-014
Part Numbers:	See Affected Part Numbers table below	***Date Issued:***	05/25/2022
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 &	ALL
H0-ECOM100 when installed in the following D0-06 series CPUs:	ALL
D0-06DD1	Firmware version prior to v2.72
D0-06DD2	Firmware version prior to v2.72
D0-06DR	Firmware version prior to v2.72
D0-06DA	Firmware version prior to v2.72
D0-06AR	Firmware version prior to v2.72
D0-06AA	Firmware version prior to v2.72
D0-06DD1-D	Firmware version prior to v2.72
D0-06DD2-D	Firmware version prior to v2.72
D0-06DR-D	Firmware version prior to v2.72

Summary

AutomationDirect is aware of vulnerabilities in the products listed above:

Vulnerability Type:

- #1: DoS Vulnerability: A specially crafted packet can be sent continuously to the PLC to prevent access from DirectSoft and other devices.
- #2: Password access: A specially crafted packet can be sent to the PLC via Ethernet to access the password

Vulnerability Classification

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

Product Advisory

Remediation

- #1: Remediation for Vulnerability (DoS) described above requires following the items listed in the next section named “Mitigations”.

- #2: Remediation for Password access: Upgrade D0-06 CPUs listed in the Affect Products section with the following firmware:

Firmware version 2.72 or later:
https://cdn.automationdirect.com/static/firmware/D06v272.zip

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.

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-D06-015
Part Numbers:	See Affected Part Numbers table below	***Date Issued:***	05/25/2022
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
D0-06DD1	Firmware version prior to v2.72
D0-06DD2	Firmware version prior to v2.72
D0-06DR	Firmware version prior to v2.72
D0-06DA	Firmware version prior to v2.72
D0-06AR	Firmware version prior to v2.72
D0-06AA	Firmware version prior to v2.72
D0-06DD1-D	Firmware version prior to v2.72
D0-06DD2-D	Firmware version prior to v2.72
D0-06DR-D	Firmware version prior to v2.72
D0-06DD2-D	Firmware version prior to v2.72
D0-06DR-D	Firmware version prior to v2.72

Summary

AutomationDirect is aware of vulnerabilities in the products listed above:

Vulnerability Type:
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.

Product Advisory

Remediation

Upgrade the CPUs with the firmware versions listed in the “Affected Products” section that can be found at this link
https://cdn.automationdirect.com/static/firmware/D06v272.zip

All DL06 CPUs (D0-06xx) **Upgrade to firmware version 2.72 or later**

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.

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.