Product Advisory

Product Family: CLICK PLC
Part Numbers: See Affected Part Numbers Table Below
Subject: CLICK Authentication Vulnerabilities

Number: PA-C0-012
Date Issued: 5/24/2021

Description of Problem:
Multiple vulnerabilities associated with programming connections and password visibility have been identified in the CLICK PLC. These could result in unauthorized connections to the PLC using the CLICK programming software.

Products Affected:

Affected Part Numbers			
C0-10DD1E-D	C0-11DD2E-D	C0-12DRE-D	C0-12ARE-1-D
C0-10DD2E-D	C0-11DRE-D	C0-12ARE-D	C0-12DD1E-2-D
C0-10DRE-D	C0-11ARE-D	C0-12DD1E-1-D	C0-12DD2E-2-D
C0-10ARE-D	C0-12DD1E-D	C0-12DD2E-1-D	C0-12DRE-2-D
C0-11DD1E-D	C0-12DD2E-D	C0-12DRE-1-D	C0-12ARE-2-D

Mitigation:
Update the Click Programming Software and Firmware to Version 3.00 or later. Latest version of CLICK Programming Software Link:
https://www.automationdirect.com/support/software-downloads?itemcode=CLICK

Please also follow the security considerations in the CLICK user manual.
https://cdn.automationdirect.com/static/manuals/c2userm/appxa.pdf

Product Description:

CLICK PLCs are programmable logic controllers designed for controlling industrial systems. They are programmed using the CLICK Programming Software, C0-PGMSW from AutomationDirect.com.

Vulnerability Classification:

AutomationDirect rates the severity level of this Product Advisory as **HIGH.**

Technical Assistance:

If you have any questions or need further information, please send an email with your contact information to techbox@automationirect.com