Product Advisory

Product Family:	Operator Panels - C-more Micro HMI	***Number:***	PA-CM-011
Part Numbers:	See Affected Part Numbers table below	***Date Issued:***	05/10/2022
Subject:	C-more EA9 Installer and Web Server Vulnerabilities	***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 Part Numbers

Affected Part Numbers	
EA9-T6CL	Software/Firmware version prior to v6.73
EA9-T6CL-R	
EA9-T7CL	
EA9-T7CL-R	
EA9-T8CL	
EA9-T10CL	
EA9-T10WCL	
EA9-T12CL	
EA9-T15CL	
EA9-T15CL-R	
EA9-RHMI	
EA9-PGMSW	Software version prior to v6.73

Vulnerability Overview

AutomationDirect is aware of vulnerabilities in the products listed above:

Vulnerability #1: DLL Hijacking in C-More Software Installer
C-More EA9 programming software installer has a DLL vulnerability that could allow hijacking during the installation process.

Vulnerability #2: Insecure Transmission of Credentials
The C-More EA9 HMI HTTP Webserver uses an insecure mechanism to transport credentials from client to web server. Therefore, an adversary could Man-in-the-Middle the connection, obtain user credentials to the HMI web server, and login as a valid user.

Remediation

Update the C-more EA9 Series Programming Software (EA9-PGMSW) and Firmware to Version 6.73 or later which supports TLS security options for the webserver.

Latest version of C-more EA9 Series Programming Software Link:
https://www.automationdirect.com/support/software-downloads?itemcode=C-more EA9 Series

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 following mitigation for instances where systems cannot be upgraded to version 6.73 or later:

- The Webserver feature can be disabled on the HMI using the programming software.
- Place the HMI panel behind a VPN: Access to and from critical control system assets in the modern environment is usually LAN based, but still should be considered remote if the operator is traversing across different networks. Virtual Private Networking (VPN) is often considered the best approach in securing trans-network communication.

Please refer to the following link for supporting information related to security considerations. https://support.automationdirect.com/docs/securityconsiderations.pdf

Product Description

The C-more HMI products are used as Human Machine Interfaces and are primarily used for the operation of automation systems.

Vulnerability Classification

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

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.