REAL Matters
Protecting Your OT Assets and Infrastructure
ICSSbD Industrial Control Systems Secure by Design

Volume 1, Advisory #8 – June 2022

REAL Matters advisories are published to communicate cybersecurity threats and risks within the Operational Technology (OT) environment and where Critical Infrastructure vulnerabilities are identified. The purpose of this newsletter is to inform, propose suggested approaches to mitigate the risk as well as provide feedback on how Mangan Cybersecurity is approaching the issue(s) addressed.

Advisory Information

At A Glance

Issue Date:	June 29, 2022
Summary:	An uncontrolled search path element, cleartext transmission of sensitive information vulnerability is found to threaten certain Automation Direct controllers and HMI products.
Systems Impacted:	Direct Logic D0-06 controller CPUs with H0-ECOM and H0-ECOM100 with firmware versions prior to v2.72 and C-more EA9 touch screen HMI running firmware versions prior to version 6.73. *Refer to CISA advisory pages https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-03, https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-02 and https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-01 for detailed models versions*
Importance:	Moderate - High

Details

Continuously sending data packets crafted specifically to the D0-06 through the HC-ECOM modules or the controller serial module can exploit the denial-of-service threat technique and specifically crafted Ethernet data packets can cause the controller to transmit the PLC access password in the cleartext readable form. A code library (DLL) vulnerability in the development install directory can allow an attacker exploit to execute code during a firmware or program download.

The touch screen HMI product vulnerability is due to the HTTP webserver's insecure mechanism to transport credentials from client to web server. This architecture may allow an attacker to obtain the login credentials and login as a valid user.

Actions and/or Recommendations

Consider product upgrades to newer Automation Direct product series.

Upgrade to firmware Version 2.72 or later for all DL06 CPUs. This firmware version mitigates brute force attack on password access. Three incorrect password entries will result in a three hour lock out of password entry. Power cycle will allow subsequent password attempts.

The c-More EA9 touch screen HMI should upgrade to firmware Version 6.73 or later as these firmware versions TLS security options for the webserver.

Additionally, if firmware upgrades are not possible implement short term mitigations to:

- Secure the controller's and HMI physical access, isolate and air gap networks when possible.
- Disable the HMI Webserver feature using the programming software.
- Place the HMI panel behind a virtual private network (VPN) for operator remote access.

About Mangan Inc.

Mangan Inc. is a nationally-recognized Specialty Engineering, Automation, and Integration company, providing a full-range of services to the Oil & Gas, Refining, Pipeline, Chemicals, and Life Sciences Industries. Established in Long Beach, California in 1990, Mangan's multiple office locations include sites in California, Georgia, New Hampshire, North Carolina, Texas, and Louisiana. Mangan's 350+ employee-owners bring expertise, innovation, and safety as their core mission to some of the largest companies in the world.