

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [ICS/OT](#)



AutomationDirect Patches Vulnerabilities in PLC, HMI Products

By [Eduard Kovacs](#) on June 20, 2022

Share

Tweet

推荐 15



The US Cybersecurity and Infrastructure Security Agency (CISA) has informed organizations that AutomationDirect has patched several high-severity vulnerabilities in some of its programmable logic controller (PLC) and human-machine interface (HMI) products.

Cumming, Georgia-based AutomationDirect provides a wide range of industrial control systems (ICS). The company sells its devices directly in the United States and Canada, but the products are also sold to organizations in other regions of the world through international distributors.

Researchers at industrial cybersecurity firm Dragos discovered that some of the company's PLC and HMI products are affected by vulnerabilities that could allow an attacker to cause disruption and make unauthorized changes to targeted devices.

CISA has published three advisories. One of them describes two [vulnerabilities affecting C-more EA9 industrial touchscreen HMIs](#), including a DLL hijacking flaw affecting the installer and an issue related to the insecure transmission of credentials.

DLL hijacking vulnerabilities can typically be exploited by an attacker that has access to the targeted system to execute code with elevated privileges. The insecure transmission of credentials

can be exploited by a man-in-the-middle (MitM) attacker to intercept a user's credentials for the HMI web server and use them to log in to the system.

These security holes have been patched with the release of firmware version 6.73. Placing the HMI behind a VPN and disabling the web server feature reduces the risk of exploitation.

A Shodan search appears to show tens of these HMIs being exposed directly to the internet, mainly located in the United States.

Learn more about vulnerabilities in industrial systems at

[SecurityWeek's ICS Cyber Security Conference](#)

The two other advisories from CISA describe vulnerabilities in DirectLOGIC PLCs, one for serial communications and one for Ethernet communications.

Some [DirectLOGIC devices with Ethernet communication modules](#) are affected by two flaws. They can be exploited by an attacker who has access to the controller by sending specially crafted packets that cause the device to enter a denial of service (DoS) condition or to cause the controller to return its password in clear text. The password can then be used by the attacker to access the controller and make malicious changes.



The PLCs with serial communication are [affected](#) by the password disclosure vulnerability.

AutomationDirect has released firmware version 2.72 to prevent the device from leaking the password. The vendor has also added protections against brute-force attacks and it has shared some recommendations on how users can mitigate risks.

Some of the affected products have been discontinued and users have been advised to consider upgrading their devices to newer models.

The vulnerabilities identified by Dragos have been assigned the CVE identifiers CVE-2022-2003, CVE-2022-2004, CVE-2022-2005 and CVE-2022-2006.

Related: [New Vulnerabilities Can Allow Hackers to Remotely Crash Siemens PLCs](#)

Related: [New Vulnerabilities Allow Stuxnet-Style Attacks Against Rockwell PLCs](#)

Related: [High-Severity Vulnerabilities Patched in Omron PLC Programming Software](#)

Share

Tweet

推荐 15

RSS



Eduard Kovacs ([@EduardKovacs](#)) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

[Flagstar Bank Data Breach Affects 1.5 Million Customers](#)

[False Air Raid Sirens in Israel Possibly Triggered by Iranian Cyberattack](#)

[AutomationDirect Patches Vulnerabilities in PLC, HMI Products](#)

[Many OT Security Incidents Result in Outages Posing Physical Safety Risk: Fortinet Staffing Firm Robert Half Says Hackers Targeted Over 1,000 Customer Accounts](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

sponsored links

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

[2022 Singapore/APAC ICS Cyber Security Conference\]](#)

 **Tags:**

[ICS/OT](#) [NEWS & INDUSTRY](#) [Vulnerabilities](#)

Search

Get the Daily Briefing

BRIEFING

Business Email Address

Subscribe



[Most Recent](#) [Most Read](#)

- [Cyberint Scores \\$40 Million Late-Stage Investment](#)
- [RevealSecurity Raises \\$23M for Application Detection and Response](#)
- [Flagstar Bank Data Breach Affects 1.5 Million Customers](#)
- [From Basecamp to Icefall: Secure by Design OT Makes Little Headway](#)
- [False Air Raid Sirens in Israel Possibly Triggered by Iranian Cyberattack](#)
- [Do Privacy and Data Protection Regulations Create as Many Problems as They Solve?](#)
- [French Encryption Firm Cosmian Raises \\$4.4 Million](#)
- [AutomationDirect Patches Vulnerabilities in PLC, HMI Products](#)
- [Germany's Green Party Says Email System Hit by Cyberattack](#)
- [QNAP Appliances Targeted in New DeadBolt, eCh0raix Ransomware Campaigns](#)

Popular Topics

- [Cybersecurity News](#)
- [IT Security News](#)
- [Risk Management](#)
- [Cybercrime](#)
- [Cloud Security](#)
- [Application Security](#)
- [Smart Device Security](#)

Security Community

- [Virtual Cybersecurity Events](#)
- [Webcast Library](#)
- [CISO Forum](#)
- [ICS Cyber Security Conference](#)
- [IT Security Newsletters](#)
- [InfosecIsland.Com](#)

Stay Intouch

- [Twitter](#)
- [Facebook](#)
- [LinkedIn Group](#)
- [Cyber Weapon Discussion Group](#)
- [RSS Feed](#)
- [Submit Tip](#)
- [Security Intelligence Group](#)

About SecurityWeek

- [Team](#)
- [Advertising](#)

- [Event Sponsorships](#)
- [Writing Opportunities](#)
- [Feedback](#)
- [Contact Us](#)

Wired Business Media

Copyright © 2022 Wired Business Media. All Rights Reserved. [Privacy Policy](#)