Product Advisory

Product Family:	Do-More H2 PLC	***Number:***	PA-DM-002
Part Numbers:	H2-DM1E	***Date Issued:***	9/26/2024
Subject:	H2-DM1E 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

Part Number	Affected Versions
H2-DM1E	All

Summary

AutomationDirect is aware of vulnerabilities in the product listed above:

- **CVE-2024-43099** - Authentication Bypass by Capture-replay:
  The session hijacking attack targets the application layer's control mechanism, which manages authenticated sessions between a host PC and a PLC. During such sessions, a session key is utilized to maintain security. However, if an attacker captures this session key, they can inject traffic into an ongoing authenticated session. To successfully achieve this, the attacker also needs to spoof both the IP address and MAC address of the originating host which is typical of a session-based attack.
- **CVE-2024-45368** - Session Fixation:
  The H2-DM1E PLC's authentication protocol appears to utilize either a custom encoding scheme or a challenge-response protocol. However, there's an observed anomaly in the H2-DM1E PLC's protocol execution, namely its acceptance of multiple distinct packets as valid authentication responses. This behavior deviates from standard security practices where a single, specific response or encoding pattern is expected for successful authentication.

Mitigations

As part of their ongoing risk assessment, AutomationDirect has determined that the H2-DM1E, due to its age and inherent architectural limitations, can no longer be supported within the secure development lifecycle. To address these challenges, AutomationDirect recommends the following mitigation strategies based on a thorough risk assessment:

- Upgrade to the BRX platform: Transitioning to the BRX platform is strongly advised, as it is designed to meet current security standards and is actively maintained within AutomationDirect's secure development lifecycle.
- Network segmentation and air gapping: To mitigate risks associated with the H2-DM1E, AutomationDirect recommends implementing network segmentation and air gapping. This strategy will isolate the older technology from the broader network, reducing its exposure to external threats and minimizing the impact of any security vulnerabilities.
- Deploy a StrideLinx secure VPN platform: AutomationDirect also recommends placing the system behind a StrideLinx VPN platform.

These mitigation strategies provide a comprehensive approach to managing the risks associated with the H2-DM1E while preparing for future security needs.

Please follow the security considerations in the following document:
https://support.automationdirect.com/docs/securityconsiderations.pdf

Product Advisory

Product Description

Do-more H2 CPU, 64k words ladder memory, (1) RS-232 (RJ12), (1) Ethernet (RJ45) and (1) USB B port(s), battery included.
This product was started in 2012.

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.