TLP:CLEAR



US Government Partners Urge Hardening Industrial Refrigeration and Cold Chain Monitoring Systems

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Health and Human Services (HHS), U.S. Department of Agriculture (USDA), and the Department of Transportation (DoT)—hereafter referred to as "the authoring organizations"—are aware of malicious cyber activity targeting industrial refrigeration and cold chain monitoring systems globally. Organizations in the Healthcare and Public Health, Chemical, Food and Agriculture, and Transportation Systems Sectors widely use these systems, including in refrigerated transport services, for automated and remote monitoring of temperatures, continuous temperature logging, defrost cycle management, and energy optimization.

The authoring organizations urge owners and operators to defend against this activity by using strong authentication, keeping systems updated, identifying any systems that are accessible from the internet, removing unnecessary remote access, and securing any necessary remote access.

Threat

The authoring organizations are aware of malicious cyber actors targeting electronic temperature controllers and commercial refrigeration controllers in retail grocery and cold storage facilities. The actors may exploit vulnerabilities or weaknesses in unpatched or internet-accessible controllers to remotely alter settings and force units into continuous heating and defrost cycles, which can cause widespread inventory loss and equipment hazards.

Specifically, the actors may exploit these flaws through multiple vectors:

- Authentication bypass;
- Arbitrary code injection; and
- Weak configurations.

Upon successful exploitation of the flaws, the actors could achieve the following effects:

- Change of temperature, which could:
  - Affect the service life of the system;
  - Create a fire hazard;
  - Cause loss of inventory; or
  - Indirectly harm consumers if products are consumed after unsafe storage.
- Loss of visibility into current temperatures (a denial-of-view condition).

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information, see Traffic Light Protocol (TLP) Definitions and Usage.

Mitigations

The authoring organizations urge owners and operators to immediately take the following actions. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs), developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement:

- **Eliminate public internet exposure**: Do not expose control system devices and/or systems, particularly controller panels, to the internet [CPG 3.S]. Should remote access be necessary, protect it by using a firewall or edge device and updating it to the latest version to reduce security vulnerabilities. See CISA's Internet Exposure Reduction Guidance and Defend the Edge: The Critical Importance of Edge Device Security for additional guidance on securing edge devices.
- **Isolate operational technology (OT) devices**: Create a dedicated OT virtual local area network (VLAN) to separate OT devices from business networks [CPG 3.I].
- **Enforce credential security**: Change default passwords [CPG 3.A], strengthen passwords, and implement strong password policies [CPG 3.B]. Further, implement phishing-resistant multifactor authentication wherever feasible [CPG 3.F].
- **Apply patches**: Keep device firmware up to date and establish a structured lifecycle management process to identify, retire, and replace legacy devices that are at end of life (EOL) and no longer supported by the manufacturer [CPG 2.A, 2.B]. See CISA's BOD 26-04: Implementation Guidance for Prioritizing Security Updates Based on Risk and BOD 26-02: Mitigating Risk From End-of-Support Edge Devices for additional guidance.
- **Restrict access**: Define and maintain device and IP address allowlisting, limiting access to only those devices and IP addresses authorized to make changes [CPG 3.H].
- **Have reliable backups**: Maintain current backups offsite and offline and test them [CPG 3.O].
- **Monitor and report**: Enable logging [CPG 3.Q] and regularly review logs for unexpected activity.
  - For OT assets where logs are non-standard or not available, collect network traffic and communications between the assets.
- **Review setpoint ranges**: Define and maintain reasonable setpoint limits for devices operating downstream of controllers to stay within safe ranges and establish alerting for deviations.

Resources

The authoring organizations strongly urge industrial refrigeration and cold chain monitoring system owners and operators to secure remote access to their OT systems. To strengthen system security, owners and operators should review the following resources and implement recommended mitigations:

- CISA: Primary Mitigations to Reduce Cyber Threats to Operational Technology
- CISA: Defend the Edge: The Critical Importance of Edge Device Security
- CISA: Internet Exposure Reduction Guidance
- United Kingdom's National Cyber Security Centre and Partners: Secure Connectivity Principles for OT

Contact Information

The authoring organizations recommend U.S. organizations report suspicious or criminal activity related to information provided in this fact sheet:

- Contact **CISA** via CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). For more information on reporting a cyber incident, refer to CISA's Voluntary Cyber Incident Reporting web page. File a claim with **FBI's** Internet Crime Complaint Center (IC3) or contact your local FBI field office. When available, please include the following information regarding the incident:
  - Date, time, and location of the incident;
  - Type of activity;
  - Number of people affected;
  - Type of equipment used for the activity; and
  - Name of the submitting company or organization, and a designated point of contact.
- Contact **HHS** via HHSCyber@hhs.gov or the HHS 24/7 Operations Center at 202-619-7800 for assistance mitigating potential disruptions to the delivery of healthcare resulting from health and medical supply chain impacts.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favor by the authoring organizations.