An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609270214

NCSC Advisory

Security Incidents Targeting Remote Refrigeration Controllers

03rd, November 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. 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 shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Recent cyber security incidents have highlighted significant security risks affecting remotely accessible refrigeration monitoring and control systems.

These systems are commonly deployed in commercial and industrial environments, including supermarkets, cold storage facilities, food distribution centres, and other temperature-controlled operations.

Attackers have reportedly gained unauthorised access to refrigeration controllers that are directly accessible over the public internet. Such access may allow unauthorised individuals to view or modify system configurations, potentially disrupting normal refrigeration operations.

Organisations operating these systems are strongly advised to review their network security posture and implement appropriate measures to prevent unauthorised access.

Refrigeration controllers with management interfaces directly exposed to the internet are at increased risk of compromise. Immediate action is recommended to secure affected installations.

Products Affected

Manufacturer	Product
Danfoss	AK-SC Series
Danfoss	AK-SM Series
Copeland / Dixell	XWEB Series

Other refrigeration controllers or industrial monitoring devices with internet-accessible management interfaces may also be exposed to similar security risks.

Organisations should review all remotely accessible refrigeration equipment, regardless of manufacturer.

Recommendations

Remove Direct Internet Exposure

- Identify refrigeration controllers that can be accessed directly through public IP addresses and remove unnecessary internet exposure.
- Management interfaces should not be directly accessible from the public internet.

Implement Secure Remote Access

- Where remote monitoring or maintenance is required, access should be provided through a properly configured and secured Virtual Private Network (VPN) or equivalent protected network solution.
- As a temporary measure, firewall rules may be configured to restrict access to known and authorised service-provider IP addresses. However, IP-based filtering alone should not be considered a permanent security solution.

Review Equipment Configurations

- Inspect refrigeration controller settings to identify unexpected or unauthorised modifications.
- Particular attention should be given to:
    - Temperature setpoints and operating parameters.
    - Defrost schedules and intervals.
    - Alarm configurations and notification settings.
    - Remote access permissions and user accounts.
- Any suspicious configuration changes should be investigated and corrected by authorised personnel.

Apply Security Updates and Strengthen Authentication

- Ensure that refrigeration controllers are running the latest appropriate manufacturer-supported firmware.
- Default passwords should be replaced with strong, unique credentials.
- Where supported, enable enhanced security settings, such as Strict Mode on applicable Danfoss controllers.

Review End-of-Life Equipment

- Identify devices that are no longer supported by the manufacturer or no longer receive security updates.

- Such equipment should be isolated from untrusted networks and assessed for replacement or additional protective controls.

For further on securing Operational Technology please see the NCSC guidance here: https://www.ncsc.gov.ie/pdfs/Securing_Operational_Technology.pdf