An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611130306

NCSC Advisory

New Vulnerabilities in Refrigeration Controllers

13 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

This advisory follows on from the NCSC's advisory of 03 November 2026 on security incidents targeting remote refrigeration controllers.

Incidents affecting internet-exposed refrigeration management interfaces have continued across Europe. Attacks began in France on 11 October 2026, with a second wave from 2 November 2026. These incidents involve internet-exposed management interfaces, including Danfoss, Dixel xweb, and Copeland xweb devices. Reported effects include unwanted defrost cycles, stock destruction and supply disruption.

Separately, published research by Midnight Blue reports six previously unknown pre-authentication remote code execution (RCE) vulnerabilities in Danfoss AK-SM800A controllers, in firmware up to and including 5.3.2. An attacker could gain full control of an affected device without valid credentials.

At the time of publication, CVE identifiers have not been assigned, no patches are available, and coordinated disclosure with the vendor is ongoing. The research also reports a flaw in the "Strict" session-control mode, and warns that an attacker could establish persistence that survives a factory reset or firmware update, or render the device inoperable.

Organisations should not rely on firmware updates, password changes or Strict Mode alone to protect an internet-exposed controller.

Products Affected

Manufacturer	Product
Danfoss	AK-SM800A (firmware up to and including 5.3.2)
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 face similar risks. Organisations should review all remotely accessible refrigeration equipment regardless of manufacturer.

Recommendations

Remove Direct Internet Exposure (only real solution)

- 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.

Note: Updating firmware, changing default passwords, and enabling strict session control are insufficient on their own to secure internet-exposed 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 guidance on securing Operational Technology, please see the NCSC guidance here: https://www.ncsc.gov.ie/pdfs/Securing_Operational_Technology.pdf

References

https://ccb.belgium.be/advisories/warning-six-new-danfoss-vulnerabilities-refrigeration-controllers-risk-immediate-action

https://www.midnightblue.nl/blog/multiple-rce-danfoss-aksm800a