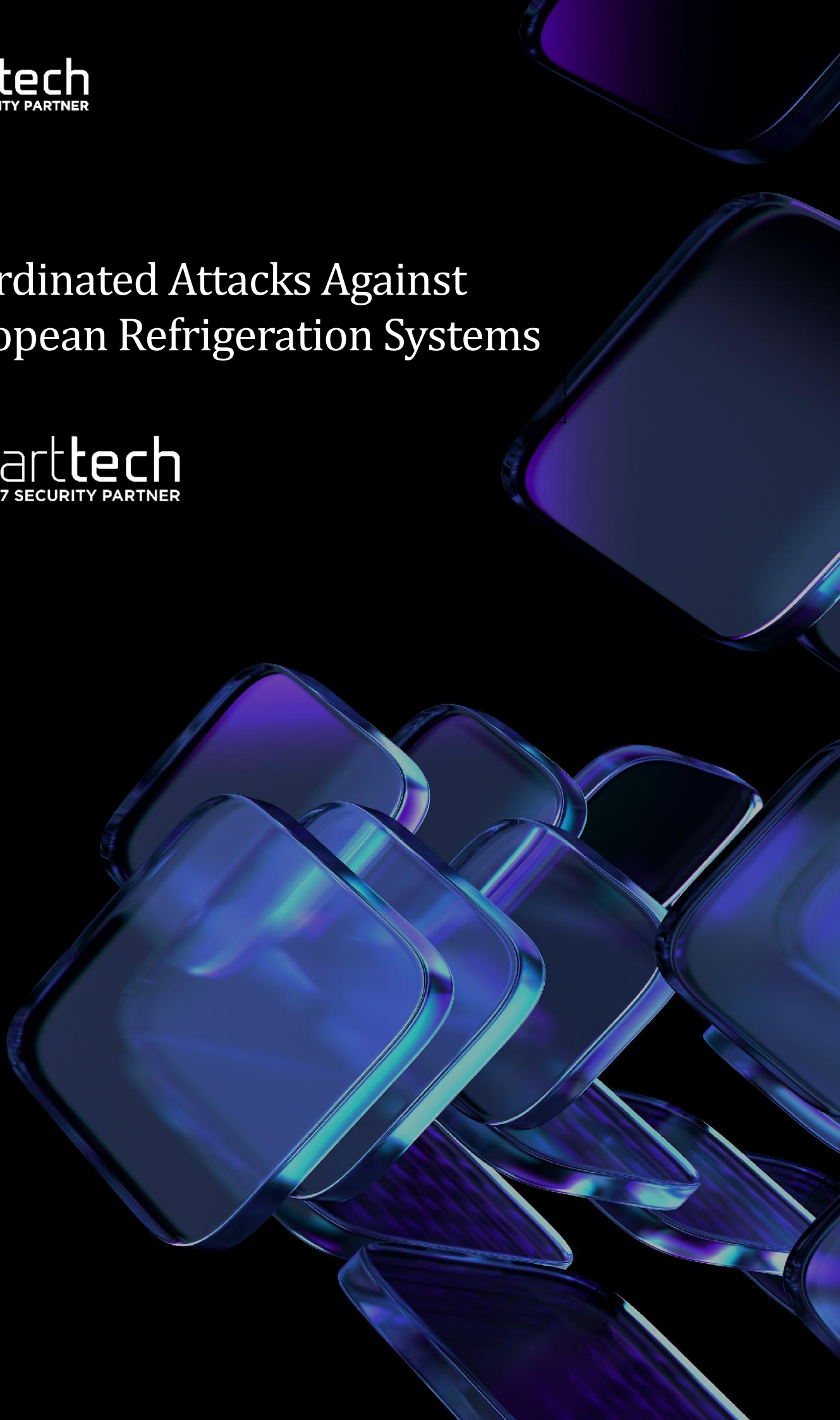
Smarttech
YOUR 24/7 SECURITY PARTNER

Coordinated Attacks Against European Refrigeration Systems

Smarttech
YOUR 24/7 SECURITY PARTNER



Executive summary

European retailers and food-sector organizations are experiencing a series of cyber incidents targeting remotely managed refrigeration systems. Attackers have manipulated refrigeration controller settings, including temperature setpoints and defrost schedules, disrupting cooling operations and causing the loss or withdrawal of temperature-sensitive goods.

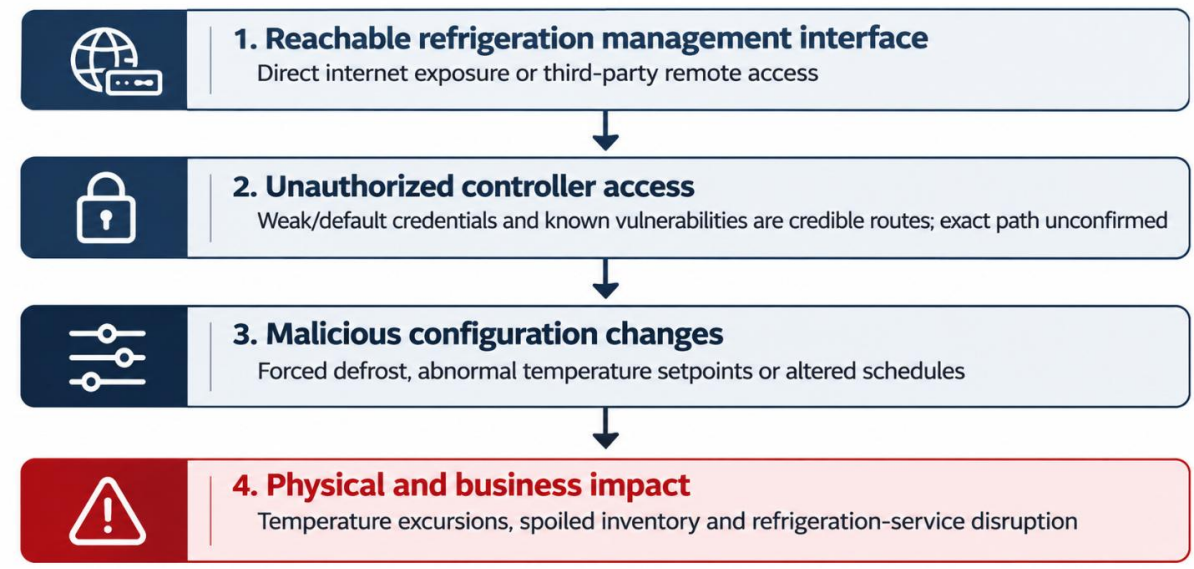
The first major publicly documented wave occurred in France on 11–12 October 2026. A renewed wave on 1–2 November affected organizations across multiple European countries. By 3 November, Euronews had identified incidents in nine countries; subsequent reporting also described incidents in Germany and limited effects within the United Kingdom's food-processing sector.

The French national cybersecurity agency, CERT-FR, has confirmed numerous compromises involving remotely managed refrigeration controllers from Danfoss, Copeland and Dixell. Its security alert, CERTFR-2026-ALE-012, warns that exploitation campaigns may remain active, particularly against end-of-life devices exposed to the public internet.

Technical Summary

The incidents involve unauthorized manipulation of refrigeration management systems. A supervisory controller can manage numerous refrigeration units, exposing functions that allow authorized operators to modify equipment settings remotely.

A plausible attack sequence, consistent with reported behavior, is illustrated below. The precise initial access method has not been independently established for every incident.



Important distinction: Reports of controllers being configured to 50°C do not necessarily mean that every affected refrigeration unit physically reached that temperature.

The following CVEs affect technologies within the identified refrigeration-controller ecosystem. Their inclusion establishes technical exposure, not proof that they were exploited in the October or November attacks.

CVE ID	Description
CVE-2025-41450	Improper authentication in Danfoss AK-SM 8xxA controllers, potentially enabling authentication bypass and exposure of sensitive system information. Affects versions before 4.2.
CVE-2025-41451	OS command injection through alarm-to-email configuration fields in Danfoss AK-SM 8xxA. May allow authenticated remote code execution. Affects versions before 4.3.1.
CVE-2025-41452	Improper control of the web server configuration in Danfoss AK-SM 8xxA. May permit authenticated denial-of-service activity. Affects versions before 4.3.1.
CVE-2026-25085	Authentication-bypass vulnerability in Copeland XWEB Pro controllers, potentially allowing unauthenticated access to administrative API functionality.
CVE-2026-21718	Predictable administrator credential-generation mechanism in Copeland XWEB Pro controllers. May allow attackers to reconstruct privileged credentials.

Claroty Team82 additionally documented multiple command-injection vulnerabilities in Copeland XWEB Pro devices, forming part of a broader set of 23 disclosed vulnerabilities.

Operators should not assume that applying a firmware update alone is sufficient. Previously compromised credentials, unsafe network configurations or unauthorized parameter changes may persist as separate risks.

Timeline

Date	Development
9 Aug 2026	Claroty Team82 publishes research on vulnerabilities and internet exposure affecting Danfoss AK-SM 800A and Copeland XWEB Pro systems.
11–12 Oct 2026	Refrigeration incidents affect hundreds of French retail locations. Remote controller manipulation leads to temperature excursions and food losses.
12 Oct 2026	CERT-FR issues alert CERTFR-2026-ALE-012.
13 Oct 2026	CERT-FR expands its alert to include Copeland and Dixell xWEB systems.
16 Oct 2026	CERT-FR strengthens its recommendations and warns that exploitation campaigns may still be ongoing.
1–2 Nov 2026	A new wave of refrigeration incidents affects retailers and other food businesses across multiple European countries.
3 Nov 2026	Further incident reporting includes Italy and Portugal; separate reporting identifies Germany and UK food-sector impacts.
3 Nov 2026	The European Commission confirms coordination meetings involving ENISA, Europol, EU-CyCLONe and affected national authorities. It declines to attribute the incidents to any actor.

No validated campaign-specific IoC list was identified in the reviewed public guidance. The absence of malware hashes is not evidence that malware could not be involved; the reported operational effects can also be produced through unauthorized configuration changes.

Recommendations and Mitigation

Organizations operating refrigeration management systems should prioritize the identification and remediation of exposed controllers, secure third-party remote access, and implement continuous monitoring for unauthorized configuration changes. Attention should be given to end-of-life equipment, outdated firmware, default credentials, and systems accessible directly from the internet.

The following measures are recommended to reduce the likelihood of compromise, limit potential operational disruption, and strengthen resilience against similar attacks.

- Identify refrigeration controllers and building management systems accessible from the public internet. Remove direct exposure of administrative interfaces and restrict remote management to secured VPN connections or appropriately segmented management networks. Where immediate remediation is not feasible, source-IP allowlisting may be applied as a temporary measure but should not be considered a permanent security control.

- Replace default, weak, or potentially compromised credentials associated with refrigeration controllers and remote management platforms. Review privileged accounts, remove unnecessary access, and enforce multi-factor authentication on remote-access gateways wherever supported. Restrict third-party maintenance access to authorized personnel and approved operational requirements.

- Inspect temperature setpoints, defrost schedules, alarm thresholds, and other critical operational parameters for unauthorized modifications. Restore approved configurations where necessary, in coordination with refrigeration engineers and service providers.

- Review available authentication records, remote-access logs, controller events, and configuration histories for suspicious activity. Where compromise is suspected, preserve relevant evidence and follow vendor-supported recovery procedures before restoring normal connectivity.

- Coordinate containment activities with site operations and refrigeration contractors to avoid unintentionally disrupting temperature monitoring, maintenance access, or critical refrigeration functions. Before disconnecting contractor-managed systems, assess potential operational, contractual, and insurance implications.

- Identify affected controllers and deploy the latest vendor-approved firmware, following compatibility validation and established OT change-management procedures. For Danfoss AK-SM 800A and affected Copeland XWEB Pro systems, verify the appropriate security updates against current manufacturer guidance.

- Prioritize the replacement of end-of-life refrigeration controllers, particularly Danfoss AK-SM 800 and AK-SC 355 devices, which no longer receive regular security updates. Network isolation should be maintained as an interim safeguard where immediate replacement is not possible.

- Separate refrigeration controllers and other operational technology from corporate IT networks and publicly accessible infrastructure. Permit only explicitly authorized communication between controllers, monitoring platforms, and remote maintenance systems.

- Disable unnecessary services and accounts, restrict administrative functions, apply the strongest vendor-supported security settings, and maintain approved configuration baselines.

- Monitor refrigeration controller activity, remote-access sessions, and critical operational parameters for suspicious behavior. Prioritize detection of unauthorized configuration changes, unexpected defrost cycles, abnormal temperature setpoints, and unusual administrative access. Integrate available controller and network logs into centralized security monitoring platforms where technically feasible.

- Review remote-access arrangements with refrigeration contractors and technology providers. Implement controlled access gateways, session logging, least-privilege permissions, and periodic access reviews.

Important: Firmware updates and factory resets should not be considered sufficient standalone remediation measures. Organizations must also address insecure network exposure, compromised credentials, unauthorized configuration changes, and unsupported equipment to reduce the likelihood of subsequent compromise.

Beyond immediate technical remediation, organizations should address the broader operational and governance risks associated with remotely managed refrigeration systems.

OT asset visibility and lifecycle management: Maintain an accurate inventory of refrigeration controllers, management platforms, firmware versions, network exposure, and third-party dependencies. Identify unsupported devices and establish a risk-based replacement program, prioritizing systems whose compromise could cause significant business interruption or product loss.

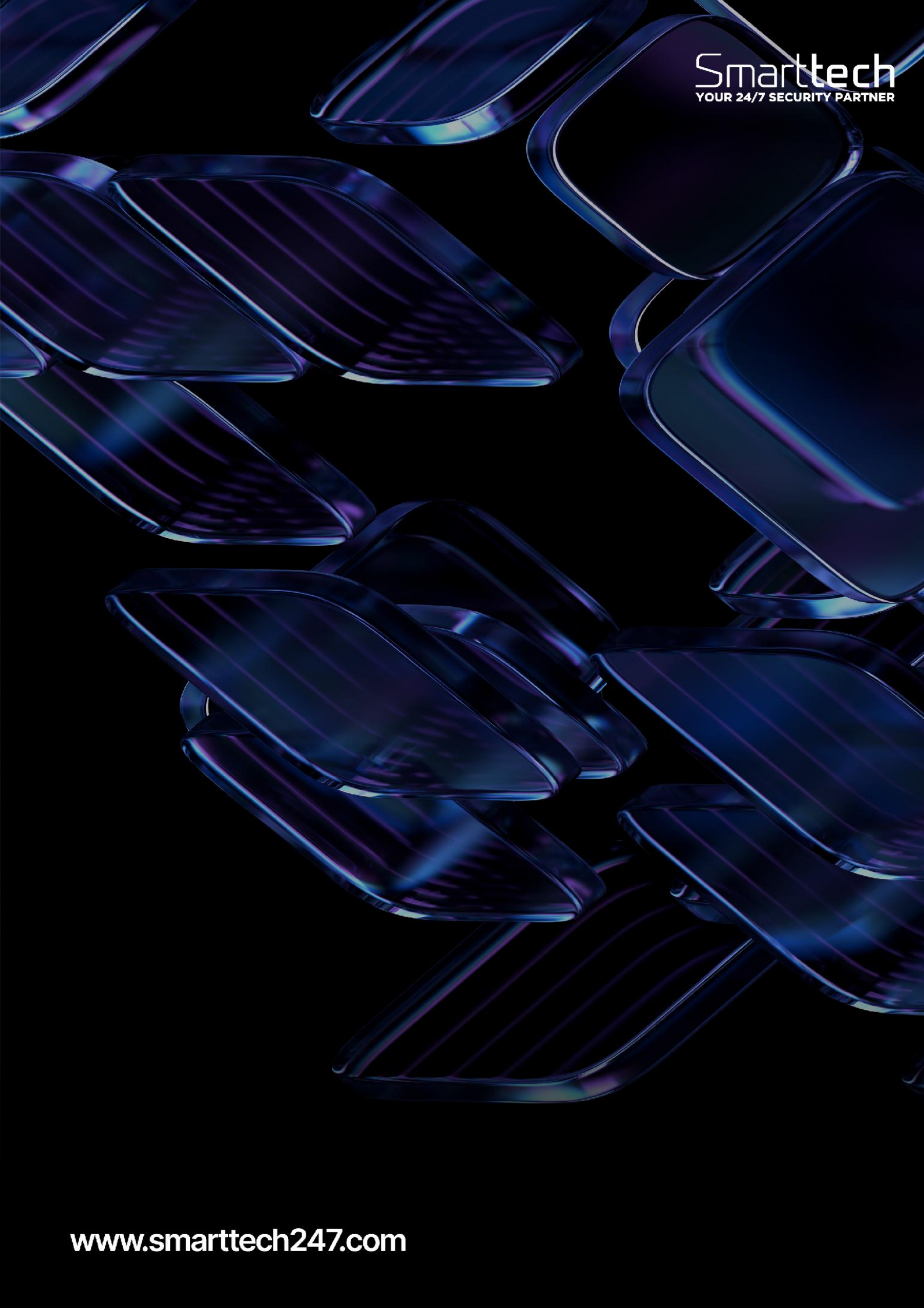
Third-party security governance: Establish minimum cybersecurity requirements for refrigeration contractors and maintenance providers, including secure remote access, credential management, vulnerability remediation, access monitoring, and incident notification obligations. Clearly define responsibility for maintaining, monitoring, and securing contractor-managed equipment.

Incident response and business continuity: Extend existing incident response and business continuity procedures to address cyber-induced refrigeration failures. Response plans should define coordination between cybersecurity teams, OT engineers, refrigeration contractors, site operations, food-safety personnel, and relevant external stakeholders.

Procedures should cover the isolation and recovery of compromised controllers, preservation of forensic evidence, manual temperature monitoring, assessment of potentially affected inventory, and alternative refrigeration or storage arrangements where required.

References

https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/
https://www.danfoss.com/en/service-and-support/downloads/dcs/adap-kool-software/ak-sm-800a/
https://www.danfoss.com/en/service-and-support/articles/dcs/tech-insider-october-2025/
https://claroty.com/blog/france-supermarket-hacks-expose-risks-of-internet-facing-refrigeration-systems
https://www.reuters.com/business/european-retailers-hit-by-supermarket-fridge-hack-2026-11-02/
https://www.euronews.com/2026/11/03/which-countries-in-europe-have-been-hit-by-supermarket-fridge-cyber-incidents
https://audiovisual.ec.europa.eu/en/media/video/I-297083
https://www.itv.com/news/2026-11-03/uk-meat-processing-firms-hit-amid-fridge-and-freezer-cyber-attacks
https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/



Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com