ISS GLOBAL / ISS GLOBAL INSIGHT REPORT

When the cold chain becomes a cyber target

European supermarket refrigeration attacks: the renewed wave and the investigative problem

REPORTING / REVIEW WINDOW

French reference wave: 11-12 October 2026; renewed European reporting: 2 November; evidence cutoff 15:26 GMT, 2 November 2026

ISSUE DATE

2026-11-02

Cyber interference with refrigeration controls can turn remote access into food withdrawal, waste and business interruption. The renewed European reports show that control integrity, equipment lifecycle and physical consequence must be investigated together.

This fresh edition examines today's developing European refrigeration incidents against the French October reference wave. It separates official technical findings, retailer acknowledgements, supplier observations and analytical hypotheses.

The investigative aim is a defensible account from controller change to measured physical effect and documented loss, with practical implications for Dfuze records.

01 / EXECUTIVE SUMMARY

What happened and its threat significance

COUNTRIES / REGION

France, Belgium, Luxembourg, Sweden, Estonia and Ireland

WHERE

Supermarket refrigeration systems and their remote supervision. Country references do not identify exact outlets or intrusion infrastructure.

WHEN

French reference wave overnight 11-12 October 2026. New incidents reported on 2 November. Evidence cutoff: 15:26 GMT, 2 November 2026.

What happened

Retailers and suppliers reported renewed refrigeration disruption across Europe. Carrefour Belgium acknowledged limited impact at 15 stores; Musgrave reported a cyber incident affecting 13 SuperValu stores; Selver confirmed one affected outlet. [3] [5] [4]

Threat significance

ISS Global assessment: unauthorised changes to operational controls can create physical and economic loss without a conventional data breach. The consequences depend on detection speed, recovery capability and actual temperature exposure.

> EXECUTIVE JUDGEMENT
>
> Prioritise protected remote access and supported equipment, while recording each installation, control change, temperature observation and loss decision as linked evidence. Maintain actor attribution as an open investigative question.

02 / THE DEVELOPING STORY

A second wave turns a French incident into a European exposure problem

Overnight on 1-2 November, retailers and refrigeration contractors reported new failures of temperature control across several European countries. The pattern resembles October's French attacks, but a common perpetrator or shared intrusion path has not been established in the reviewed record.

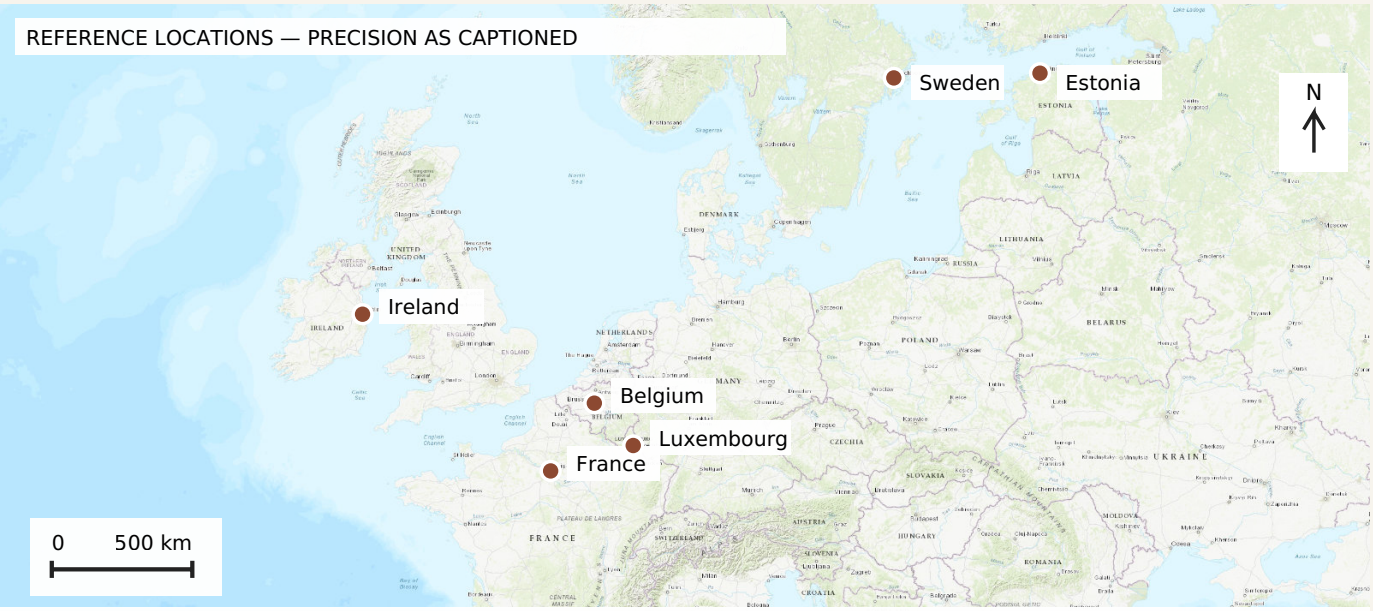
Reuters gathered accounts from Delhaize, Colruyt, ICA and refrigeration suppliers; Sweden's national cybersecurity centre said it was working on several grocery-refrigeration incidents. Reports range from acknowledged IT disruption to explicit cyberattack descriptions. These differences matter: one chain's confirmed wording cannot upgrade every other case. [2]

France supplies the earlier reference point. AP reported that the finance minister estimated about 700 affected supermarkets and that prosecutors were investigating food losses and possible fires. Initial counts varied with reporting time and inclusion rules. This report retains the attributed estimate without treating it as a verified event-by-event register. [6]

DATE	DEVELOPMENT	EVIDENCE TREATMENT
11-12 Oct	French refrigeration disruptions emerge	Original event period; later store counts are revisions.
12-16 Oct	CERT-FR issues and revises technical alert	Primary record of affected product families and response advice. [1]
1-2 Nov	New European disruptions reported	Multiple country/store records; campaign linkage remains an assessment.
2 Nov	Retailer and supplier updates continue	This edition is frozen at 15:26 GMT; it is not a final loss assessment.

03 / GEOGRAPHY

Reported footprint, without invented store locations



Map 1. Country reference points for France, Belgium, Luxembourg, Sweden, Estonia and Ireland. Capital markers identify countries, not affected stores or attacker infrastructure. Esri topographic basemap and listed contributors; WGS84 / Web Mercator; 500 km independently checked scale. Acquired 2 November 2026.

Geographic spread shows a shared exposure class, not a proven transnational command structure. An affected national retail group can contain franchised stores, contractor-managed equipment and locally maintained controllers. Each installation requires its own configuration, ownership and evidence record.

The map deliberately omits exact outlets, control servers and network paths. These were not consistently established. Additional countries mentioned in isolated or restricted reports are excluded from the core register pending stronger supporting records.

04 / COUNTRY AND OPERATOR REGISTER

The reported counts describe different populations

COUNTRY / OPERATOR	REPORTED SCOPE	STATUS AND CONSEQUENCE
France / multiple chains	About 700 supermarkets, ministerial estimate	October reference wave; food losses and possible fires investigated. [6]
Belgium / Carrefour	15 of more than 700 stores	Direct statement: limited impact, no hypermarkets, stores remain open. [3]
Belgium / Spar	Five franchised shops	Colruyt account reported by Reuters; retain separately from other chains. [2]
Belgium and Luxembourg / Delhaize	Dozens of stores across reporting	IT incident and temperature increases acknowledged; no defensible country split. [2]
Sweden / Coop and ICA	Six Coop stores; limited ICA number	Retailer reports and individual store accounts differ in attribution strength. [2]
Estonia / Selver	One outlet confirmed	Supplier reports rapid intervention; no product damage reported. [4]
Ireland / SuperValu	13 stores	Musgrave confirms cyber incident and precautionary chilled/frozen withdrawal. [5] [10]

Do not add these values as a European total. They mix dates, estimates, geographic groupings and outcome definitions. Stores affected, units compromised, stock withdrawn and confirmed spoiled stock are separate measures.

> COMPARABILITY RULE
>
> A defensible total needs a unique outlet identifier, observation cutoff, event membership and a clear definition of affected. None of the reviewed sources supplies a complete cross-country denominator.

05 / TECHNICAL EVIDENCE

Compromised refrigeration supervision is established; the exploit chain is not

CERT-FR reports numerous compromises involving Danfoss AK-SM and AK-SC families and Copeland/Dixell XWEB supervision. It warns against exposing management interfaces directly to the internet. This supports an operational-technology compromise assessment; it does not identify one exploit for all affected premises. [1]

Danfoss's published advisory table lists authentication-bypass CVE-2025-41450 for AK-SM8xxA before 4.2, and post-authentication CVE-2025-41451/41452 before 4.3.1. These are relevant inventory checks, not confirmed exploitation indicators for this wave. [7]

LAYER	WHAT THE EVIDENCE ESTABLISHES	WHAT REMAINS SEPARATE
Exposure	Remote refrigeration management exists; CERT-FR reports compromises.	Public exposure, credential misuse and contractor access must be checked per installation.
Control action	Operators and suppliers describe altered temperature or defrost behaviour.	An authenticated configuration change needs event logs or a competent examination.
Physical effect	Some stores withdrew food; others recovered without reported damage.	Setpoint is not measured cabinet air temperature or product-core temperature.
Attribution	The reviewed reporting does not establish a perpetrator.	Sabotage, extortion and state involvement are hypotheses requiring evidence.

ISS Global assessment: trusted control functions can produce harmful consequences when abused. The incident should be investigated as a control-integrity failure with physical effects, not reduced to whether conventional data theft occurred.

06 / CONSEQUENCE CHAIN

The temperature headline conceals several different facts

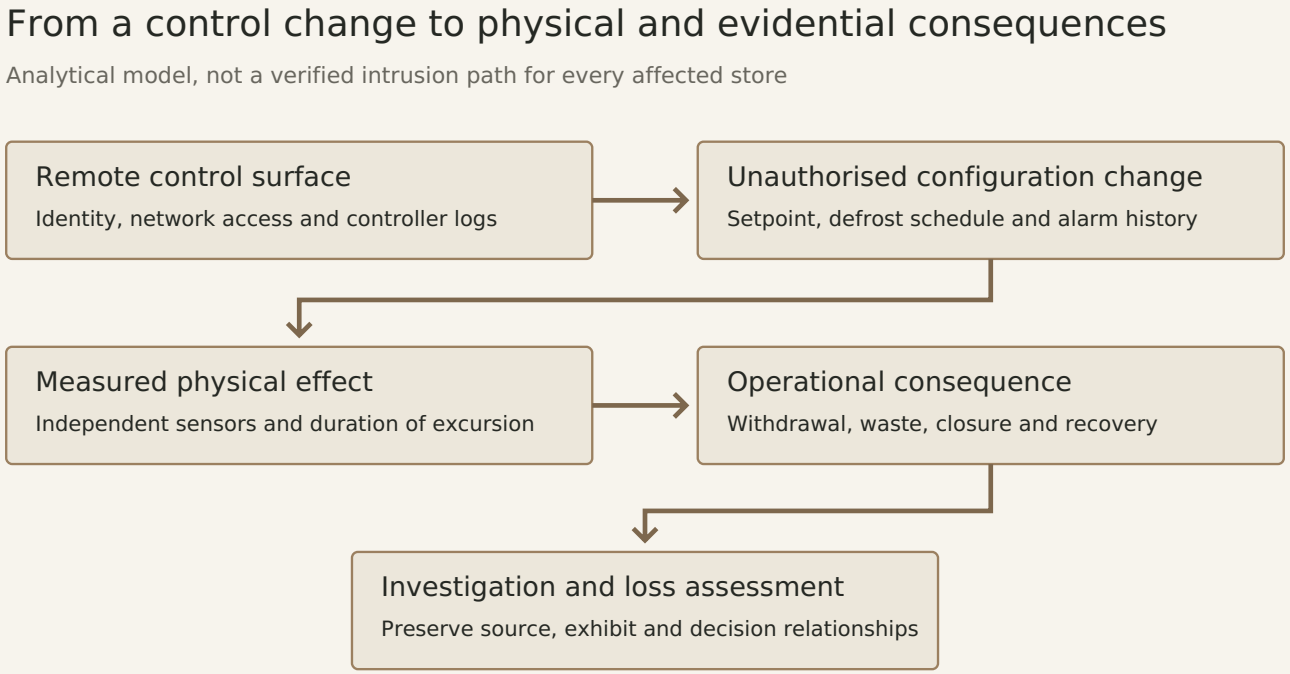


Figure 1. ISS Global analytical model. It organises collection questions and does not assert a verified intrusion path at every store.

At the Estonian Selver outlet, Kitman reported a 50°C setting but an actual rise of only about two to three degrees before intervention. Normal temperature reportedly returned within roughly 10-15 minutes and no product damage was reported. [4]

The contrast is investigative, not merely semantic. A changed command, sensor reading, duration of exposure, product-safety decision and disposal certificate can support different propositions. A complete case preserves all five, including their clocks and measurement conditions.

07 / RESPONSE AND CONTINUITY

Protect cooling while preserving the evidence of interference

CERT-FR prioritises removing public internet exposure, restoring access through protected networks or secure VPNs, reviewing configuration and applying vendor security measures. It warns that resetting unsupported equipment alone can leave it exposed to renewed compromise. [1]

Danfoss's earlier guidance emphasises supported equipment, current software and secure installation. Product replacement addresses lifecycle risk only when the surrounding access controls are also sound. [8]

PRIORITY	OPERATIONAL OBJECTIVE	EVIDENCE REQUIREMENT
Immediate safety	Refrigeration and food-safety leads decide safe product handling and continuity.	Timestamped readings, affected batches, withdrawal decision and responsible person.
Containment	Coordinate isolation with the retailer, refrigeration specialist and incident responder.	Record changes, remote sessions and disconnection times; avoid uncontrolled loss of supervision.
Preservation	Capture proportionate logs/ configurations when safe before destructive recovery.	Original files, hashes, collection method, clock offset and chain of custody.
Recovery	Validate settings and independent temperature readings before return to service.	Approved baseline, restoration actions, testing and sign-off.
Prevention	Inventory controllers, access paths, support status and contractor responsibilities.	Versioned asset and account records; verified maintenance and replacement ownership.

These are coordination priorities, not instructions to operate a live refrigeration installation. Food preservation and safe engineering control remain the responsibility of competent operators; evidence collection should support those decisions.

08 / DFUZE INVESTIGATIVE INTELLIGENCE

Follow the installation, the claim and the physical loss

RECORD OBJECT	MINIMUM USEFUL FIELDS	WHY IT MATTERS
Incident and outlet	Store ID, country, event window, discovery, reporting date	Prevents duplicate outlet counts and false chronology.
Controller / installation	Vendor, model, firmware, support state, service contractor	Distinguishes product-family exposure from a specific exploited device.
Access event	Account, session, source, authorised purpose, timestamp basis	Tests competing credential, exposure and remote-maintenance hypotheses.
Configuration exhibit	Original export, baseline comparison, collector and hash	Supports the claimed unauthorised change.
Temperature observation	Sensor ID, value, unit, location, calibration and interval	Separates command from measured air and product conditions.
Consequence	Batch, withdrawal, disposal, downtime, cost basis and insurer	Documents physical/economic harm without inflating it.
Source and assessment	Original URL/file, claimant, status, translation and revision	Preserves reported facts and analytical inference as different states.

DFUZE DEMONSTRATION

Begin with one store record, link the controller and service provider, attach the change history, then trace each loss claim to temperature and stock evidence. A campaign view should be derived from these linked records while retaining competing assessments.

09 / ATTRIBUTION AND OUTLOOK

Repeated behaviour justifies comparison, not a common-actor conclusion

ISS Global assessment: the present record supports recurring abuse of connected refrigeration controls across several operators. Similar timing, legacy equipment and defrost manipulation justify a comparative inquiry. They do not establish the same attacker, infrastructure, access method or motive.

QUESTION	DISCRIMINATING EVIDENCE
One campaign or opportunistic repetition?	Shared infrastructure and session histories, reproducible configuration patterns and timing after clock normalisation.
Supplier route or separately exposed stores?	Access topology, contractor identity, authentication records and affected/unaffected comparisons.
Food loss or preventive withdrawal?	Temperature history, safety decision, disposal and valuation records.
Compromise continuing after recovery?	Verified access changes, configuration drift and monitored restoration evidence.

Retailer disclosures indicate materially different effects. Carrefour states that all Belgian stores remained open; Musgrave describes withdrawal at 13 stores; Selver reports no product damage after fast detection. These outcomes show why incident severity should be measured at the installation and consequence level. [3] [5] [4]

Evidence gaps and visual review

No complete cross-country event list, shared exploit proof, forensic image or authoritative attribution was reviewed. Photography located in reporting was principally retailer context or agency imagery without established reuse permissions; it is omitted. The map and consequence diagram are original analytical graphics. No generated scene is used.

This edition covers evidence available through 15:26 GMT on 2 November 2026. Later acknowledgements may change the country footprint and loss estimates. The separate October Ahold corporate IT disruption is not merged into the refrigeration cases.

SOURCE REGISTER

Sources 01–05

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

01 Incident de securite ciblant les controleurs a distance des installations de refrigeration

CERT-FR / **ANSSI** · 12 October 2026; revised 16 October

Family: French national technical alert · Accessed 2 November 2026. Full French bulletin read and translated by the assistant. Official account of compromises and affected families; it does not identify the exploit used in every store.

https://www.cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012

02 Cyberattack on fridges hits supermarkets across Europe

Reuters / **MarketScreener** · 2 November 2026

Family: Reuters interviews and operator accounts · Accessed 2 November 2026. Accessible syndicated text read. Counts and assessments attributed to chains, suppliers and Swedish cybersecurity centre; an evolving multi-country report, not a final census.

https://uk.marketscreener.com/news/european-supermarkets-hit-by-new-fridge-cyber-attack-ce785fd8d18af221

03 Impact tres limite sur les installations frigorifiques chez Carrefour Belgique

Carrefour Belgique · 2 November 2026

Family: Direct retailer statement · Accessed 2 November 2026. Full French statement read; Dutch counterpart checked. Retailer reports limited impact, 15 stores and all stores open. Both languages are one source family.

https://newsroom.carrefour.be/impact-tres-limite-sur-les-installations-frigorifiques-chez-carrefour-belgique-les-produits-restent-disponibles-et-lensemble-des-magasins-est-ouvert-oi9rj2

04 Hackers raised freezer temperature at Selver supermarket to +50 C

ERR · 2 November 2026

Family: Direct supplier and retailer interviews · Accessed 2 November 2026. Full English report read. Selver confirms one outlet; Kitman describes control change, rapid response and measured temperature rise. Technical entry method unresolved.

https://news.err.ee/1610183296/hackers-raised-freezer-temperature-at-selver-supermarket-to-50-c

05 Supervalu removes frozen and chilled food from 13 stores after cyber attack on fridges

The Irish Times / **Musgrave** · 2 November 2026, 10:15

Family: Retailer statement via local reporting · Accessed 2 November 2026. Accessible report and Musgrave statement reviewed. Specific equipment model not named. Precautionary removal is distinct from quantified spoilage.

https://www.irishtimes.com/technology/data-security/2026/11/02/supervalu-removes-frozen-and-chilled-food-from-13-stores-after-cyber-attack-on-fridges/

SOURCE REGISTER

Sources 06–10

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

06 Cyberattack targeting refrigeration systems hits 700 supermarkets

Associated Press / **ABC News** · 13 October 2026

Family: French minister, prosecutor and supplier statements · Accessed 2 November 2026. Accessible full wire text reviewed. About 700 is the ministerial estimate; same article describes a separate Ahold corporate-system incident without establishing a common cause.

https://abcnews.com/Business/wireStory/cyberattack-targeting-refrigeration-systems-hits-700-supermarkets-french-137230099

07 Danfoss security advisories: DSA-2025-03-01 and DSA-2025-08-01

Danfoss · 24 March and 1 August 2025

Family: Manufacturer vulnerability records · Accessed 2 November 2026. Official indexed advisory table reviewed; direct page access restricted. Authentication and post-authentication flaws affect specified AK-SM8xxA versions. Existence is not evidence of exploitation in these incidents.

https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/

08 Tech Insider October 2025

Danfoss · October 2025

Family: Manufacturer operational security guidance · Accessed 2 November 2026. Manufacturer indexed article reviewed. Supports lifecycle and protected-access context; earlier incidents are historical background, not evidence of the 2026 actor.

https://www.danfoss.com/en/service-and-support/articles/dcs/tech-insider-october-2025/

09 Recommandations pour une utilisation securisee des superviseurs XWEB, v1.0

Dixell · October 2026

Family: Manufacturer guidance linked by CERT-FR · Accessed 2 November 2026. Reference identified through the official CERT-FR bulletin; not relied upon for unreviewed technical detail.

https://dixell.fr/wp-content/uploads/2026/10/Recommandations-pour-une-utilisation-securisee-des-superviseurs-XWEB-v1.0.pdf

10 SuperValu pulls chilled and frozen food from sale in 13 stores after cyberattack

The Journal / **Musgrave** · 2 November 2026

Family: Same Musgrave statement family as source 5 · Accessed 2 November 2026. Accessible statement reviewed. No named stores or restoration deadline in the company statement. Repetition does not create independent corroboration.

https://www.thejournal.ie/supervalu-cyber-incident-13-stores-fridges-7212412-Nov2026/