ZEROFOX INTELLIGENCE

Flash

European Supermarket Refrigeration Cyberattacks

F-2026-11-04a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Vulnerability, Threat Actor, Geopolitical

November 4, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EST) on November 3, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | European Supermarket Refrigeration Cyberattacks

| Key Findings

- On November 2, 2026, supermarkets in Belgium, Luxembourg, Sweden, Ireland, and Estonia reported refrigeration failures apparently caused by cyberattacks, and reporting indicates the Netherlands and Finland were also affected. No actor has claimed responsibility as of the time of writing.
- ZeroFox assesses that the most significant impacts to date are likely disruption to retailer operations and a decline in consumer confidence in the food supply rather than a decrease in food availability.
- ZeroFox assesses that further attacks will likely occur in the coming weeks targeting additional European retailers and other sectors reliant on remotely managed refrigerated supply chains, such as food distribution, cold storage, and healthcare.
- ZeroFox assesses it is likely that these incidents will increase regulatory and insurer scrutiny of operational technology (OT) and third-party remote access in the retail and food supply sectors and reinforce the use of cyberattacks that cause visible physical effects in order to erode public trust in essential services.

© 2026 ZeroFox, Inc. All rights reserved.

Overview

On November 2, 2026, supermarkets in Belgium, Luxembourg, Sweden, Ireland, and Estonia reported refrigeration failures apparently caused by cyberattacks, and reporting indicates the Netherlands and Finland were also affected.[1] No actor has claimed responsibility as of the time of writing. ZeroFox has moderate confidence that the incidents are linked and assesses that further attacks are very likely.

- In several cases, attackers reportedly raised refrigeration temperatures to 50°C, forcing retailers to discard stock.[2]

Details

Modern supermarket refrigeration is commonly managed through central controllers with web interfaces, allowing store staff and third-party maintenance firms to monitor circuits and adjust temperature settings remotely.[3] On the night of October 11–12, attackers forced defrost cycles on these controllers across hundreds of French stores, with temperatures reportedly held near 50°C for about six hours.[4] The attackers reportedly did not deploy malicious code on the controllers, which complicates attribution.[5]

On November 2, the activity expanded, with Carrefour reporting 15 of more than 700 Belgian stores were affected;[6] Sweden's ICA and Coop, Ireland's Musgrave (13 SuperValu stores), and an Estonian Selver outlet also reported incidents.[7] An ICA Kvantum store reported its units were set to 50°C, and an Estonian refrigeration supplier said attackers accessed a computer controlling a client's system. Separately, citing four officials, Reuters reported that the Pentagon suspects August freezer outages that occurred at

[1] hXXps://www.aljazeera[.]com/news/2026/11/3/very-cold-war-whos-attacking-europes-supermarket-freezers
[2] hXXps://abcnews[.]com/International/wireStory/freezers-supermarkets-european-countries-hit-apparent-cyberattacks-137765494
[3] *Ibid.*
[4] hXXps://www.incibe[.]es/en/incibe-cert/publications/cybersecurity-highlights/cyberattack-supermarket-refrigeration-systems-france
[5] hXXps://www.cnn[.]com/2026/10/14/europe/france-cyberattack-supermarket-fridges-intl
[6] hXXps://abcnews[.]com/International/wireStory/freezers-supermarkets-european-countries-hit-apparent-cyberattacks-137765494
[7] hXXps://gizmodo[.]com/supermarket-freezers-across-europe-hit-with-another-cyberattack-2000833828

© 2026 ZeroFox, Inc. All rights reserved.

two U.S. military facilities are the work of hackers and that investigators are in contact with French authorities. No link between the U.S. and European incidents has been established to date.

Impact

ZeroFox has observed reports of destroyed fresh and frozen stock across multiple countries, with French losses reportedly in the millions of euros and some refrigeration units overheating to the point of fires or melting.[8] Recovery has varied: Musgrave stated its incident was fully resolved on November 2 with restocking under way, and the Estonian supplier said its incident was addressed within minutes.[9] The European Commissioner for Agriculture and Food stated that food security is not currently at risk but that food waste and business impact are real.[10] ZeroFox assesses that the most significant impacts to date are likely disruption to retailer operations and a decline in consumer confidence in the food supply rather than a decrease in food availability.

Outlook and Assessment

ZeroFox assesses there is a roughly even chance that the October and November incidents are linked, given the shared technique (temperatures raised to 50°C), similar target class (remotely managed supermarket refrigeration), and escalation across borders within three weeks. ZeroFox has not observed reporting of a ransom demand and assesses that the activity is more consistent with disruption than financial gain. The actor's identity and affiliation remain unknown, and ZeroFox cannot attribute the attacks to a specific actor with any confidence at this time. It is unlikely that formal public attribution will occur within the next 30 days, as the attackers reportedly left no malicious code on the controllers.

ZeroFox assesses that further attacks will likely occur in the coming weeks targeting additional European retailers and other sectors reliant on remotely managed refrigerated supply chains, such as food distribution, cold storage, and healthcare. The technical barrier is likely low, as affected systems were reportedly internet-accessible, running unsupported firmware, or protected by weak credentials, and ZeroFox assesses that publicity is likely to attract opportunistic copycat activity. More broadly, ZeroFox

[8] hXXps://www.aljazeera[.]com/news/2026/11/3/very-cold-war-whos-attacking-europes-supermarket-freezers
[9] *Ibid*.
[10] hXXps://www.politico[.]eu/article/european-commission-probe-supermarket-cyberattack-christophe-hansen/

© 2026 ZeroFox, Inc. All rights reserved.

assesses it is likely that these incidents will increase regulatory and insurer scrutiny of OT and third-party remote access in the retail and food supply sectors and reinforce the use of cyberattacks that cause visible physical effects in order to erode public trust in essential services.

Recommendations

ZeroFox recommends that retailers, food distributors, cold-storage operators, and any organization reliant on remotely managed refrigeration take the following actions, in priority order:

- Inventory remote refrigeration controllers. Identify all system managers and controllers, including the Danfoss AK-SM and AK-SC and Copeland/Dixell XWEB devices named by CERT-FR (the French national and governmental Computer Emergency Response Team) and the third-party maintenance connections that reach them.
- Remove internet exposure. Take administrative interfaces off the public internet, and restrict access to trusted network segments or secured remote access with multi-factor authentication.
- Eliminate weak access. Change default and guessable passwords, and apply available vendor firmware updates.
- Replace end-of-life units. Prioritize replacement of discontinued controllers that no longer receive security updates, and isolate them in the interim.
- Audit third-party access. Review which maintenance and managed service providers hold remote access, enforce unique credentials per provider, and log all remote sessions.
- Detect and contain. Alert on unauthorized setpoint or defrost changes using temperature sensors and alarms independent of the controller network, and maintain a tested manual override and stock-relocation plan.
- Report and share. Notify the national CERT or relevant authority of suspected incidents and monitor CERT-FR and equivalent agency guidance for updates.

© 2026 ZeroFox, Inc. All rights reserved.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

© 2026 ZeroFox, Inc. All rights reserved.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

© 2026 ZeroFox, Inc. All rights reserved.