Shop fridges and freezers across Europe hit by fresh suspected cyber-attack

Chains in seven countries say cooling unit temperatures rose overnight in incident similar to hack of French shops

Jon Henley, *Guardian*, 2 November 2026 (shortened)

Supermarket chains in at least seven European countries have said the temperatures of refrigerators and freezers in some of their shops soared overnight to as high as 50C (122F), echoing a cyber-attack last month that caused millions of euros of damage in France.

Retailers in Belgium, Estonia, Ireland, Finland, Luxembourg, the Netherlands and Sweden reported problems with their refrigeration systems on Monday, and several companies confirmed they had been hacked.

The EU food and agriculture commissioner, Christophe Hansen, said the repeated cyber-attacks were deeply concerning, calling them "a deliberate attempt to disrupt our food supply chain and undermine consumers' confidence in it".

The incidents follow an attack in France last month in which hackers seized control of cooling units in as many as 700 supermarkets, raising their temperatures as high as 50C (122F) and causing fires and food losses estimated in the tens of millions of euros.

A growing range of devices, including refrigeration systems, can now be monitored and controlled remotely, leading authorities to particularly fear government-sponsored hybrid attacks after Russia's 2022 invasion of Ukraine.

Many cyber-attacks involve extortion or are politically motivated and are potentially carried out by state-level actors, said Tom Hegel of the cybersecurity firm SentinelOne. But the supermarket attacks, with no financial demands, point to sabotage, he said.

"Retail is an easy target because retail chains run enormous estates of refrigeration controllers, building management systems, door access panels and point-of-sale gear," Hegel told Reuters.

Patrick Lamplmair of the cybersecurity firm Tributech said cyber-attackers would keep going "until it stops working" because the method was "cheap and the damage is immediate". Many refrigeration systems had known and as yet unfixed flaws, he said.

"Thousands of these controllers were still reachable from the internet after the French attack," he added. "A few commands to a temperature controller can destroy stock overnight and close stores."

In the French attack, the hackers pirated controllers mostly supplied by the Danish company Danfoss, which said subsequently that it had identified some security flaws last year and had "long recommended" customers install updates.

The hackers remotely overrode the settings on thousands of freezers, fridges and chiller cabinets at chains including Intermarché, Coopérative U, Carrefour, Leclerc and Monoprix, pushing them from as low as -27C to well over 50C.

The shops had to discard vast quantities of fresh meat, dairy and frozen products. Individual supermarkets reportedly suffered losses ranging from tens of thousands of euros to more than €130,000 (£109,000).

The Paris prosecutor's office has opened a formal investigation into the French attack and the prime minister, Sébastien Lecornu, instructed France's national cybersecurity agency, Ansii, to investigate.

The agency subsequently reported that supermarkets using controllers from two other companies had also been targeted in the attack, but authorities have not indicated who could have been behind the incidents. There have been no claims of responsibility.