Refrigeration Controls Tampered With at European Supermarkets, Forcing Stores to Pull Food



Attackers remotely changed refrigeration control settings at supermarkets in Belgium, Sweden, Estonia and other European countries, warming fridges and freezers. Some stores discarded or withdrew chilled and frozen food.

- The changes were made remotely overnight into Monday, November 2.
- Supermarkets in Belgium, Sweden, Estonia and other European countries were affected.
- No chain reported more than several dozen affected stores.
- Some stores threw away or removed chilled and frozen food from sale.
- Danfoss, a Danish maker of refrigeration controls, is named in the report.

What happened

According to The Hacker News, attackers remotely altered the settings of refrigeration controls at supermarkets in Belgium, Sweden, Estonia and other European countries. The changes were made overnight into Monday, November 2, and caused fridges and freezers to warm.

No chain reported more than several dozen affected stores. Some stores had to throw away chilled and frozen food or take it off the shelves. The report names Danfoss, a Danish maker of refrigeration controls; the portion of the source available to us does not detail the attack method or the company's response.

Why it matters for regulated institutions

The incident shows how tampering with operational technology can cause physical and commercial loss without any data being stolen. Cold-chain equipment such as refrigeration controllers is often managed remotely, and it can sit outside the scope of routine IT security reviews.

Organisations in the Kingdom that operate retail, food, healthcare, pharmaceutical or logistics facilities, or that finance and insure them, may hold similar exposure through building and refrigeration systems.

What to do next

Treat this as a prompt to review remote access to refrigeration and building controls, and to confirm that temperature monitoring and manual fallback procedures work independently of the control network.

What to do now

1. Inventory refrigeration and building controllers across stores, warehouses and cold-chain sites, including who can reach them remotely.
2. Restrict remote access to these controllers, require strong authentication, and remove direct internet exposure.
3. Install independent temperature monitoring with alerts that does not rely on the control system itself.
4. Ask refrigeration and facility vendors about security advisories, updates and remote-access practices for their controllers.
5. Rehearse a manual fallback and stock-disposal procedure for a temperature excursion, and include it in business continuity plans.