

Remote attack on Danfoss refrigeration controllers warms fridges at French supermarkets



Attackers remotely took over Danfoss refrigeration controllers at hundreds of French supermarkets on the night of October 11, warming fridges and freezers and forcing stores to discard food.

- Hundreds of French supermarkets were affected on the night of October 11, according to several retail chains.
- Attackers warmed fridges and freezers, and stores had to throw away food.
- The entry point was the Danfoss controller that runs all refrigeration in a store.
- Maintenance firms can manage this controller remotely, which made remote access the path in.

What was reported

On the night of October 11, attackers took remote control of refrigeration equipment at hundreds of French supermarkets. Fridges and freezers were deliberately warmed, and several retail chains said they had to throw food away.

How access was gained

The attackers reached the equipment through the controller that manages all of a store's fridges and freezers. The device is made by the Danish company Danfoss, and maintenance firms can administer it remotely. The source does not detail the technique used, so this should be treated as a case of remote maintenance access to operational technology being abused, not as a confirmed software flaw.

Why it matters for Saudi institutions

The incident shows that a single building-level controller can turn a cyber intrusion into physical loss: spoiled stock, disrupted trading and waste. Retailers, food distributors, hospitals, pharmacies and cold-chain operators in the Kingdom often rely on similar controllers and on third-party maintenance providers with remote access. The sensible response is calm and practical: know where such devices are, who can reach them, and how quickly temperature deviations would be noticed.

What to do now

1. Inventory refrigeration and building controllers, including those managed by third-party maintenance firms.
2. Review which vendors have remote access, and require MFA, named accounts and time-limited sessions.
3. Ensure these controllers are not directly reachable from the internet and are segmented from corporate networks.
4. Set independent temperature monitoring and alerts that do not rely on the controller itself.
5. Include cold-chain failure in business continuity and incident response plans, with a stock-loss decision procedure.