France Attributes Refrigeration Controller Sabotage at About 700 Retail Sites to Iran



France says an IRGC cyber unit altered defrost settings on refrigeration controllers at about 700 retail sites on October 11, causing food losses and at least 15 fires. Operators of connected cooling systems should review exposure.

- The French government attributes the attack to a cyber unit of Iran's Islamic Revolutionary Guard Corps.
- Attackers accessed refrigeration controllers at about 700 retail sites on the night of October 11.
- They set defrost settings to high temperatures.
- The result was food losses and fires in at least 15 cases.

What happened

The French government has stated that an October cyberattack on refrigeration controllers at about 700 retail sites was carried out by a cyber unit of Iran's Islamic Revolutionary Guard Corps (IRGC). According to the report, the intruders gained access to the controllers on the night of October 11.

Once inside, they changed the defrost settings to high temperatures. The physical consequences were food losses and, in at least 15 cases, fires.

Why it matters

This is a case of sabotage aimed at physical equipment through its control layer, not data theft. Refrigeration controllers are common in retail, food distribution and logistics, and they are often managed remotely and sit outside the focus of conventional IT security programmes. The reported outcome shows that a settings change alone can create safety and financial harm.

The source excerpt does not describe the access method, the controller vendor or any technical indicators, so we do not draw conclusions on those points.

What to do next

Institutions in the Kingdom with retail, food or cold-chain operations should treat building and refrigeration controllers as operational technology within their risk register. A calm, practical review of inventory, remote access and alerting for setting changes is a sensible first step, alongside confirming incident procedures cover physical safety events.

What to do now

1. Inventory refrigeration and building controllers across sites, including who can reach them remotely.
2. Remove direct internet exposure and require VPN with multi-factor authentication for remote management.
3. Change default credentials and restrict vendor access to approved, time-limited sessions.
4. Alert on changes to temperature and defrost settings and set hard safety limits on the equipment.
5. Add physical-impact scenarios such as fire and stock loss to incident response and business continuity plans.