

Cyberattack Advisory: Iranian Attack on French Supermarket Refrigeration

10 November 2026 · Chris Harper, Chief Security Officer

Attacks on Connected Equipment

On November 9, 2026, the French government formally blamed Iran for an October 12 cyberattack that took remote control of refrigeration systems in about 700 supermarkets across France. Temperatures inside the units reached 50 degrees Celsius (122 degrees Fahrenheit) for roughly six hours, forcing stores to throw out fresh and frozen goods, and one chain reported losses of tens of millions of euros in a single day. France's national cybersecurity agency attributed the attack to the Shahid Kaveh group, a cyber unit affiliated with Iran's Islamic Revolutionary Guard Corps, and French officials described it as the first large-scale sabotage attack on French soil.

The activity does not appear to be limited to France or supermarkets. A separate attempt to overheat storage at several French blood banks was stopped last week before it could cause damage, and supermarkets in Sweden, Belgium, Luxembourg, Ireland, and Estonia have reported freezer and refrigerator failures that also appear to have been caused by cyberattacks. Coming after this summer's attacks on Minnesota water systems, which investigators tentatively linked to Iran, it adds to a pattern of Iranian-affiliated groups going after the internet-connected equipment that keeps everyday operations running.

Risk to SMBs come from HVAC, door access, camera systems and other IoT devices that are often installed and maintained by outside vendors, or in the case of IoT devices end users themselves. Many are frequently managed through remote-access portals and left out of regular IT security reviews. Knowing which of these systems in your environment can be reached from the internet and taking precautionary measures can help reduce the chance that this kind of equipment is used against you.

It is recommended that IoT devices be given separate network access, segregated from primary network devices, and the IoT inter access be restricted to only those services which are required to perform their primary function. Additionally, any default access password should be changed, and SNMP community strings should have the PUBLIC string changed for something unique. It is also recommended that external penetration tests be performed annually and cyber liability insurance be reviewed for coverage.

If you would like Sandbox Technologies to review the connected equipment in your environment or discuss your current security and AI assisted penetration testing, please respond to this email to reach me directly. We will review your environment and advise you on next steps.

Further information is available via the links provided below.

- ABC News (AP): France Blames Iran for Last Month's Cyberattack on Supermarket Fridges
- Al Jazeera: France Accuses Iran of Cyberattack on Supermarket Fridges
- Al-Monitor: France Vows Tough Response to Freezer Cyberattack Blamed on Iran

Ref. Iranian-Linked Sabotage of French Supermarket Refrigeration Systems, October 2026

Sincerely,
Chris Harper
Chief Security Officer
Sandbox Technologies, Inc.