Version 2 · Public summary

Exposed refrigeration controllers in France

What internet scan data shows after the supermarket attacks of 11 to 12 October 2026

14 October 2026 · ACDS Security Research Group

Summary

Overnight on 11 to 12 October 2026, attackers took remote control of refrigeration controllers in several hundred French supermarkets and forced display cases into continuous defrost. CERT-FR has confirmed numerous compromises of Danfoss AK-SM and AK-SC controllers, and on 13 October extended its alert to Copeland xweb and Dixell xweb controllers.

We analysed 30 days of internet-wide scan data for Danfoss AK-SM 800A controllers whose web management interface can be reached from the internet, and measured how that exposure changed after the CERT-FR alert.

~2,300
AK-SM 800A controllers in France reachable from the internet (30 days to 13 Oct), on 2,292 addresses

30%
of regularly scanned French controllers were no longer visible after the alert, against 5% elsewhere

84%
of French exposed addresses sit on anonymous business broadband lines

Key findings

1. **France holds half of the world's exposure.** Around 2,300 to 2,500 French controllers were reachable on 2,292 addresses, out of 4,598 addresses worldwide. Belgium is a distant second.
2. **The exposure is spread store by store.** Almost every exposed address is a single controller behind a small business router, made reachable by port forwarding. We found no small set of contractor gateways through which most of the estate could be fixed at once. Remediation has to happen site by site.
3. **Only a minority can be attributed from public data.** About 16% of exposed addresses sit in blocks registered to a named organisation, including retail and food businesses and IT or monitoring service providers. The remaining 84% are on anonymous business broadband lines.
4. **Exposure fell sharply after the alert.** 30% of regularly scanned French controllers were no longer visible in the three days after the CERT-FR alert, against 5% in the rest of the world.

1. What happened

Drawn from public reporting and official statements as of 14 October. Sources are listed at the end.

- **Attack.** Store refrigeration controllers were taken over and defrost cycles forced to run continuously. Some display cases reportedly reached around 50 °C for several hours, and stock had to be discarded.
- **Retailers named.** Intermarché and Netto, Coopérative U, Carrefour, Monoprix and E.Leclerc. Public estimates of affected stores range from about 250 to about 500.
- **Impact.** Large food losses. Intermarché's chief executive expects losses of tens of millions of euros across France. Fires have been reported at some locations, and whether they are linked to the attack is under investigation.
- **Official response.** CERT-FR alert CERTFR-2026-ALE-012, issued 12 October and updated 13 October, covers Danfoss AK-SM and AK-SC, Copeland xweb and Dixell xweb. It names no vulnerability and publishes no indicators of compromise. The Paris prosecutor's office has opened an investigation.

- **Vendor statement.** Danfoss says most affected devices were end-of-life AK-SM 800 (end of life 2021) and AK-SC 355 (phased out 2016) units, plus some current AK-SM 800A units running outdated firmware.
- **Entry route.** Not public. Candidate routes discussed are direct internet exposure of the controller interface, a maintenance contractor's remote-access path, or the vendor's own environment.

Known vulnerabilities in the AK-SM 800A

Three vulnerabilities in the AK-SM 800A were disclosed in 2025, all reported by Claroty's Team82 research group through coordinated disclosure:

- **CVE-2025-41450**, an authentication bypass through a hidden "code of the day" login (CVSS 8.2). CISA published ICS advisory ICSA-25-140-03 on 20 May 2025. Fixed in firmware R4.2.
- **CVE-2025-41451**, command injection through the alarm e-mail settings, allowing remote code execution once logged in, and **CVE-2025-41452**, injection into the web server configuration. Danfoss published advisory DSA-2025-08-01 in August 2025. Fixed in firmware R4.3.1.

Claroty published a detailed public analysis on 9 August 2026, urging owners to update to R4.3.1 or later and to remove management interfaces from the internet. No source links these vulnerabilities to the October attack, and they affect only the AK-SM 800A, not the older models Danfoss says made up most victims. However, the AK-SM 800A is exactly the model visible in our data, and Danfoss says some compromised 800A units were running outdated firmware.

2. Method

We used commercial internet-wide scan data covering 13 September to 13 October 2026, and repeated the searches on 14 October to measure change after the alert. Organisations were identified from public internet registry records (RIPE), reverse DNS and the French company registry. Detailed scan records were reviewed for the 14 largest addresses. This brief is based only on existing scan and registry data. We did not connect to or interact with any device.

Counting controllers. The scanner revisits each device roughly every three days, so one controller produces about 10 observations in a 30-day window. We therefore count unique addresses, and estimate controllers as observations divided by 10, with a minimum of one per address. Figures mean "seen in the 30 days to 13 October", not "online now".

3. How exposed controllers can be identified

Across 197 Danfoss records reviewed in detail, the following signals identify an AK-SM 800A. They are not always present together, so any one should be treated as a match.

Signal	Value	Notes
Web page title	`Danfoss StoreView` `Danfoss - StoreView Web`	Present on 192 of 197 records. The second title is newer firmware
TLS certificate	`CN=DanfossSM800A, OU=SM800A, O=Danfoss` Variant: `CN=SystemManager`	Factory self-signed certificate; not universal
HTTP response header	`Access-Control-Allow-Headers: aksm-auth, …`	Present on most, but not all, sites
Secondary service port	TCP 1041 with the Danfoss certificate	Seen alongside the web interface on several sites

The web server is nginx, with versions varying by firmware age. Page dates and ETags differ per unit and appear to reflect firmware build dates, which could support an estimate of how many units run outdated firmware.

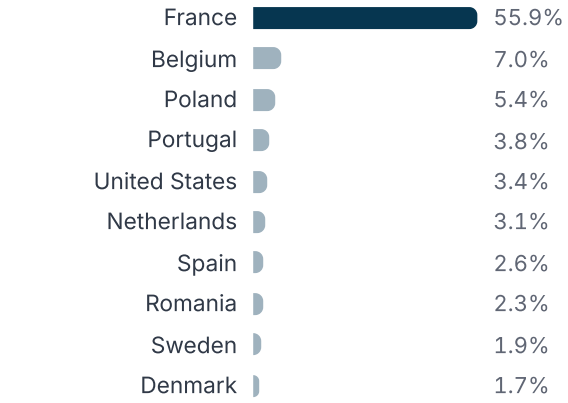
> **Not covered.** We have no reliable signal for the older AK-SM 800 and AK-SC 355 units, and we have not yet assessed Copeland xweb or Dixell xweb controllers, which were added to the CERT-FR alert on 13 October.

4. Exposure findings

Scope	Unique addresses	Estimated controllers
France	2,292	2,300 to 2,500
Worldwide	4,598	4,600 to 5,000

These are consistent with independent counts published by Claroty (2,765 AK-SM 800A worldwide) and Predicta Lab (2,752 worldwide, 1,590 in France on 12 October); our 30-day window includes devices that have since gone offline.

Share of worldwide exposure by country, top 10



Share of scan observations, 30 days to 13 October 2026. 74 countries in total.

Who holds the French exposed addresses



Carrier lines: anonymous business broadband pools (Orange alone about 58%), which only the carrier can map to a subscriber. Split is approximate: a few registry names belong to small providers.

5. Shape of the French estate

- **One controller per line.** The vast majority of addresses carry a single controller. About 140 addresses show signs of two or more.
- **Exposure by port forwarding.** Controllers sit behind small business firewalls and routers (FortiGate, Stormshield, Orange Livebox) with the controller deliberately forwarded to the internet. Two addresses that appeared to front many controllers are in fact single controllers placed in the router's DMZ, answering on every port.
- **Store IT, not contractor gateways.** The genuine multi-controller sites hold two to four controllers behind one business line, often alongside VNC remote desktop, IP cameras and building-energy controllers. This is the profile of a single store or small group's own IT.
- **The contractor route is neither confirmed nor ruled out.** Scan data cannot see a contractor's remote-access path unless the contractor also owns the address block. No contractor can be named from passive data for any address on an anonymous carrier pool.

6. Change since the CERT-FR alert

We compared devices the scanner visits regularly (at least nine observations in the baseline month) with what was seen between 11 and 14 October.

Regularly scanned controllers still visible, 11 to 14 October



France: 1,178 of 1,676. Rest of world: 1,013 of 1,067.

In France, 498 regularly scanned controllers (30%) were not seen again in the three days after the alert, against 5% elsewhere. That is about 410 more than the background rate would predict. The fall was concentrated among single-controller sites and larger organisations; sites with several controllers were almost all still visible.

"Not seen in three days" is not proof of removal, because the scan cadence is about three days. The rest of the world acts as the control. Address changes do not explain the fall.

7. Recommendations for operators

These recommendations follow CERT-FR's published guidance.

- Remove refrigeration controller management interfaces from direct internet exposure, including DMZ and port-forwarding rules on store routers. Allow remote access only through a VPN or a strict allow-list.
- Review each controller's full configuration, including defrost schedules and setpoints. Change default and shared passwords, and rotate credentials held by maintenance providers.
- Update AK-SM 800A units to firmware R4.3.1 or later, and use the strict security mode where offered.
- Where compromise is suspected, factory reset, reconfigure and restore access only over a protected path. CERT-FR notes that a reset alone is not enough for exposed end-of-life equipment, which should be isolated or replaced.

Sources

- CERT-FR, alert CERTFR-2026-ALE-012: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2026-ALE-012/
- ANSSI, alert update adding Copeland and Dixell xweb (13 Oct): https://x.com/ANSSI_FR/status/2110004485565428018
- CISA, ICS advisory ICSA-25-140-03 (20 May 2025): https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03
- Danfoss, security advisory DSA-2025-08-01: https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/dsa-2025-08-01/
- Claroty Team82, AK-SM 800A analysis (9 Aug 2026): https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers
- The Hacker News, 13 Oct 2026: https://thehackernews.com/2026/10/attackers-heat-french-supermarket.html
- Cooling Post, Danfoss statement: https://www.coolingpost.com/world-news/danfoss-moves-to-mitigate-cyberattack/
- BleepingComputer: https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-refrigerators-at-french-supermarkets/
- Batirama, 13 Oct 2026: https://www.batirama.com/article/114113-la-cyberattaque-contre-le-froid-commercial-touche-des-centaines-de-magasins.html