European Refrigeration Controller Exposure: A Second Attack Wave

Following coordinated cyberattacks on supermarket refrigeration systems in France on **October 10-11, 2026**, and a second wave across several European countries on **November 2, 2026**, Censys has tracked a sustained decline in Internet-exposed refrigeration controllers named in CERT-FR emergency alert **CERTFR-2026-ALE-012**. Across the two advisory product families, Copeland/Dixell XWEB and Danfoss StoreView, observed global exposure fell **53%**, from 6,695 to 3,124 distinct hosts, between October 9 and November 5, 2026.

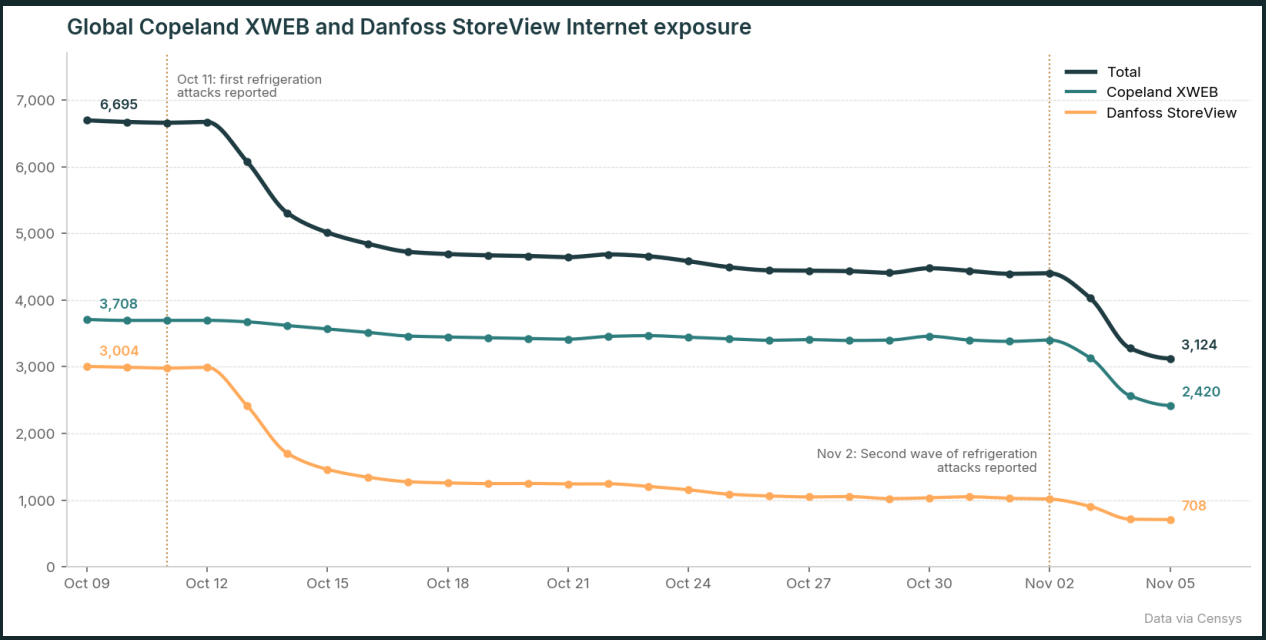
EXECUTIVE SUMMARY

- Total Internet-exposed refrigeration controllers in the two advisory families fell **53%** (6,695 to 3,124 distinct hosts) between October 9 and November 5, 2026.
- **Danfoss StoreView** exposure dropped **76%** (3,004 to 708); **Copeland/Dixell XWEB** dropped **35%** (3,708 to 2,420).
- The first, sharp decline was almost entirely **France**, where Danfoss StoreView exposure fell from 1,841 hosts to 497 over October 13-15, then eased to 209 by November 5, following the French attacks reported around October 11.
- A second, broad decline began **November 2** and affected both vendors (Danfoss down 30% across 32 countries; Copeland down 29% across 36 countries), coinciding with reported attacks in Belgium, Estonia, Ireland, Luxembourg, the Netherlands, and Sweden.

-53%
TOTAL EXPOSURE
OCT 9 TO NOV 5

-76%
DANFOSS STOREVIEW
3,004 TO 708

-35%
COPELAND/DIXELL XWEB
3,708 TO 2,420



Internet-exposed refrigeration controllers, October 9 to November 5, 2026. The total is the union of Copeland/Dixell XWEB and Danfoss StoreView hosts. Total exposure fell 53%, from 6,695 to 3,124. Dotted lines mark reported events (around October 11 and November 2), not proven causes.

BACKGROUND: TWO REPORTED ATTACK WAVES

On the night of **October 11, 2026**, attackers switched refrigeration units at hundreds of French supermarkets into defrost mode, spoiling food and, in some cases, causing fires. The targeted systems were **Danfoss StoreView** controllers with Internet-exposed management interfaces. French authorities issued emergency alert **CERTFR-2026-ALE-012**, calling for these controllers to be removed from the Internet. Public research by Claroty Team82 has shown that disclosed Danfoss vulnerabilities, including **CVE-2025-41450** (a date-based administrator login), can be chained for remote code execution.

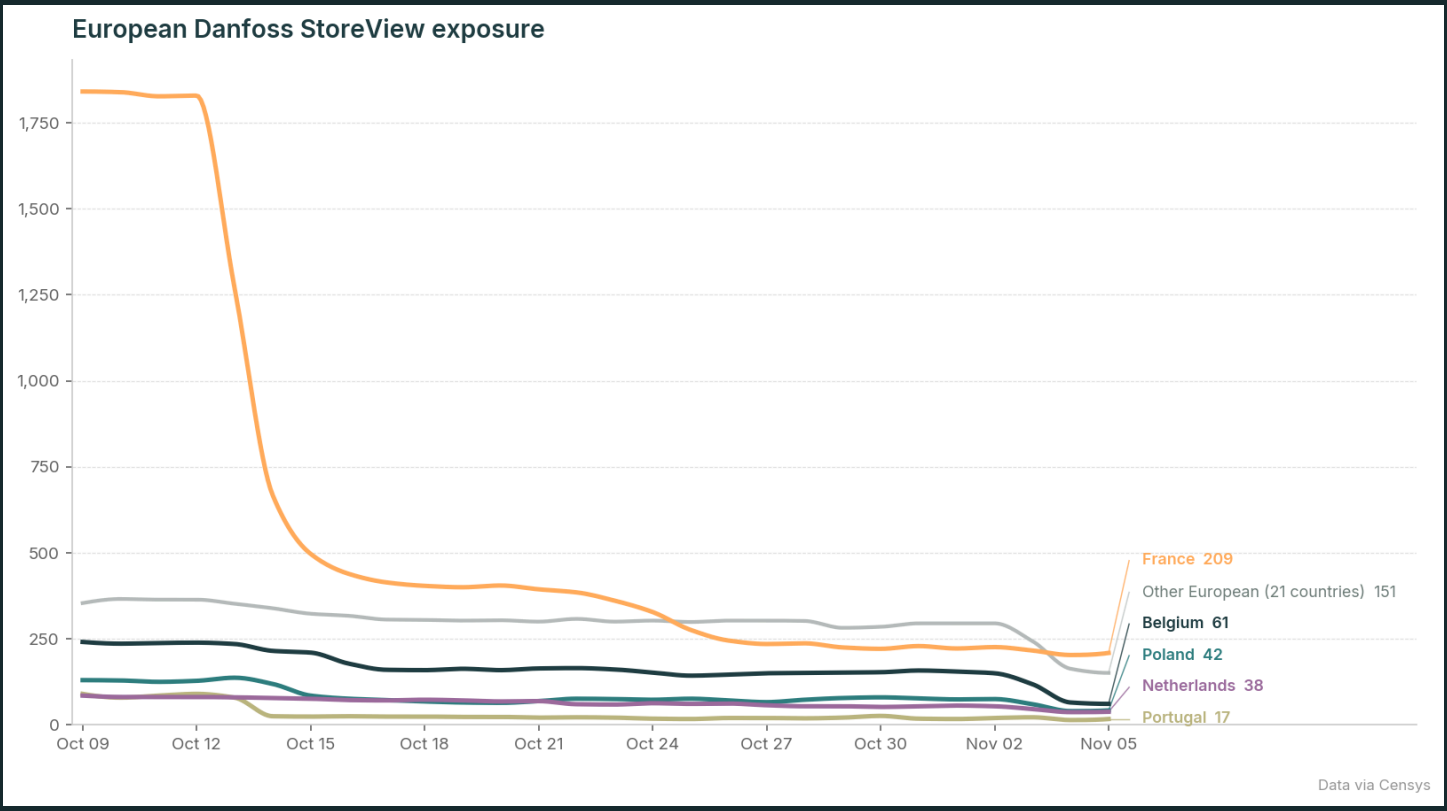
Overnight on **November 2, 2026**, grocers and small shops in **Belgium, Estonia, Ireland, Luxembourg, the Netherlands, and Sweden** reported a second wave, with attackers remotely raising case temperatures. No group has claimed responsibility, and it is not confirmed that the same actor was behind both waves.

ADVISORY AND VULNERABILITIES

Danfoss disclosed **CVE-2025-41450** in March 2025, an unauthenticated administrator login derived from the current date, followed by **CVE-2025-41451** and **CVE-2025-41452** in August 2025, which allow authenticated command execution and disruption of the management interface. Public research by Claroty Team82 later showed the first two could be chained for remote code execution. CERT-FR emergency alert **CERTFR-2026-ALE-012** calls for these controllers to be removed from the Internet.

DANFOSS STOREVIEW: CONCENTRATION

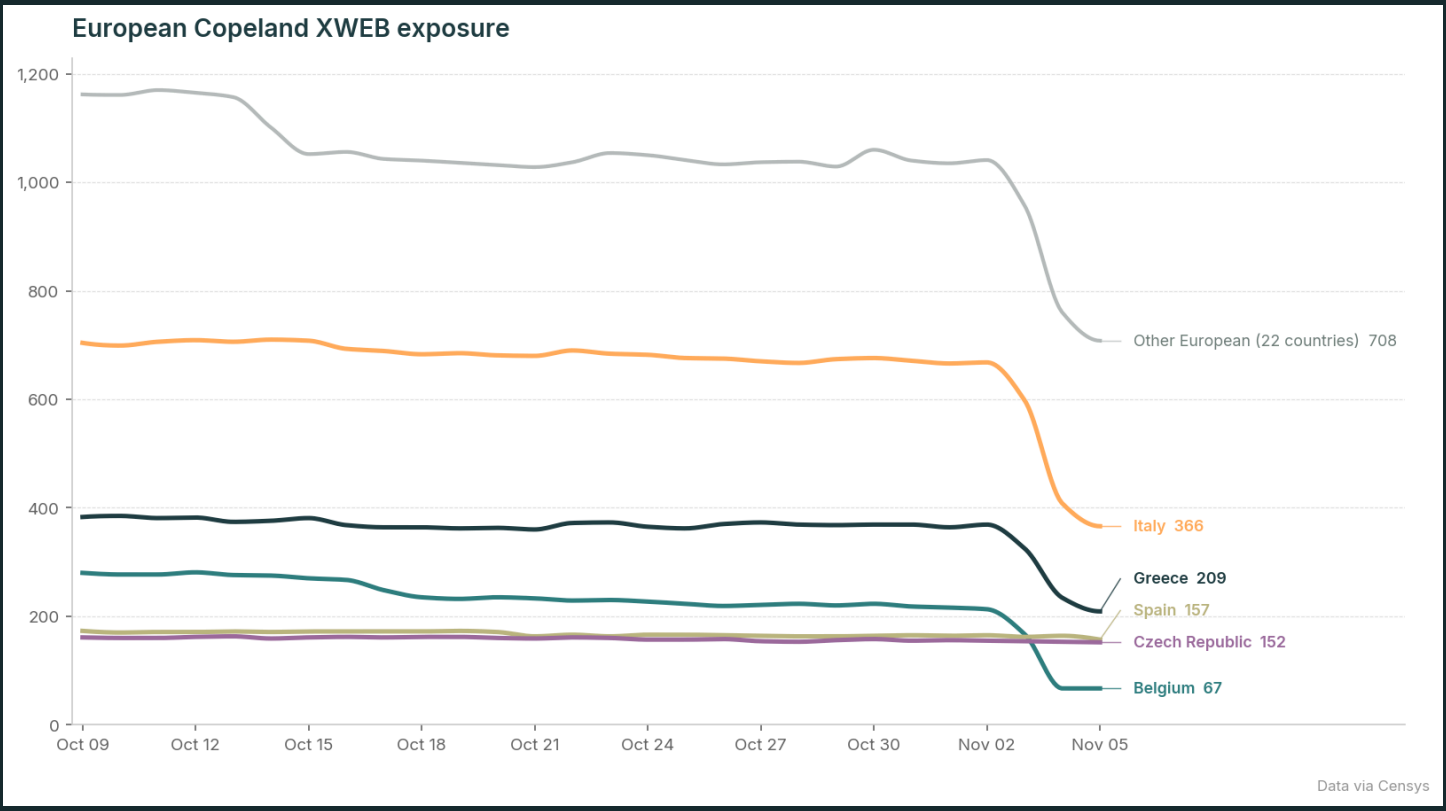
As of **November 5, 2026**, Danfoss StoreView exposure remains concentrated in France (209 hosts) and Belgium. France alone accounted for the bulk of the vendor's global total before the October attacks and still leads the European distribution after a 76% fall.



Danfoss StoreView exposed hosts by European country, October 9 to November 5, 2026. The top five countries by October 9 exposure are drawn in color; every other European country is summed into one line. France dominates, falling from 1,841 to 209 hosts; the French step (October 13-15) precedes a further broad decline after November 2.

COPELAND/DIXELL XWEB: A LONG TAIL

Copeland/Dixell XWEB exposure is distributed across a long tail of mid-sized countries, led by Italy (366) and Greece (209), unlike the France-centric Danfoss picture. Most of Copeland's decline came after November 2: its exposure was roughly flat through late October, then fell about 29% across 36 countries in the final days of the window.



Copeland/Dixell XWEB exposed hosts by European country, October 9 to November 5, 2026. Italy leads (366). The summed "other European" line (708) is the largest series, reflecting a long tail of mid-sized countries rather than one dominant country. Copeland exposure held through October, then fell sharply after November 2.

CENSYS ASSESSMENT

Between October 9 and November 5, 2026, Internet-exposed hosts in the two advisory families fell 53% (6,695 to 3,124). The decline came in two distinct moves. The first, on October 13-15, was almost entirely France, where Danfoss StoreView exposure dropped from 1,841 to 209 hosts, overlapping the French attacks reported around October 11. The second began on November 2 and was broad: Danfoss fell 30% across 32 countries and Copeland/Dixell XWEB fell 29% across 36 countries over the final days of the window. The data does not show why the controllers went offline. A fall in exposure is consistent with provider action or owners disconnecting devices, and these measurements do not distinguish among them.