

Forum:[Hack Forums](#)

Thread: [Hackers Turned French Supermarket Fridges Into Heaters](#)

Bastille - October 12, 2026, 1:07 pm

Hackers Turned French Supermarket Fridges Into Heaters

Hundreds of stores affected, and security researchers had already demonstrated serious vulnerabilities in refrigeration controllers.

[Video: <https://www.youtube.com/watch?v=UxxtjKAsyWk>]

Something pretty crazy happened here in France during the night of October 11–12, 2026.

Several major supermarket chains, including Intermarché, Carrefour, Coopérative U and Monoprix, were reportedly hit by a cyberattack targeting their refrigeration systems.

And instead of stealing data or deploying ransomware, the attackers apparently managed to manipulate refrigeration equipment remotely.

Some refrigerators reportedly reached temperatures of 50°C (122°F), causing massive food losses, equipment damage and even reports of fires.

Basically, hackers managed to turn supermarket fridges into heaters.

But here's where the story gets even more interesting.

Researchers had already demonstrated vulnerabilities in these systems

In August 2026, cybersecurity researchers from Claroty Team82 published a technical investigation into vulnerabilities affecting Danfoss AK-SM 800A refrigeration controllers.

These controllers are designed to monitor and manage commercial refrigeration equipment remotely.

The researchers discovered several security issues, including:
CVE-2025-41450: Authentication bypass involving a daily access code.

CVE-2025-41451: OS command injection potentially allowing remote command execution.

CVE-2025-41452: Nginx configuration injection, potentially leading to denial of service.

Their research involved firmware analysis, reverse engineering and investigation of the controller's authentication mechanisms.

They also demonstrated how these weaknesses could be combined to compromise a vulnerable

controller.

Technical write-up:

Very detailed article here : [Claroty Team82 – Freeze the Controller, Defrost the Food: Uncovering Vulnerabilities in Danfoss Refrigeration Controllers](#)

If you're interested in reverse engineering, embedded systems or OT security, I definitely recommend reading it.

What about a video demonstration?

The research was also presented at DEF CON 34 in August 2026 by Amir Zaltzman.

I haven't found a publicly confirmed video showing the complete exploitation chain yet, but you can look for the conference presentation here:

[DEF CON 34 – Danfoss Refrigeration Security Research](#)

The Claroty article itself is already a pretty interesting technical demonstration, with details about the vulnerabilities and how they were discovered.

Important: Although these vulnerabilities affect the same family of refrigeration controllers reportedly involved in the French incident, there is currently no public confirmation that the attackers exploited these specific CVEs.

What happened to the supermarkets?

According to initial reports, several hundred stores were affected across France.

Some refrigeration systems reportedly remained at abnormally high temperatures for hours, forcing supermarkets to dispose of large quantities of food.

Stores had to temporarily shut down refrigerated sections, and some reportedly experienced equipment damage or fires.

The Paris prosecutor's office has opened an investigation, and French cybersecurity authorities are looking into the incident.

The attackers' identities and exact intrusion methods have not yet been publicly confirmed.

Why I find this case fascinating

We often talk about ransomware, stolen credentials, leaked databases and compromised websites.

But this is a completely different situation.

We're talking about attackers potentially manipulating physical equipment through vulnerable industrial control systems.

And the consequences aren't limited to the digital world anymore: food safety issues, financial losses, damaged equipment and potentially dangerous situations.

It's also a good reminder that a device doesn't need to store sensitive information to become an attractive target.

Sometimes, simply being able to control what a device does is enough.

Sources

[Claroty Team82 – Technical vulnerability research](#)

[Reuters – Cyberattack targeting French supermarkets](#)

[Le Monde – Cyberattack against supermarket refrigeration systems](#)

I'm curious what you guys think.

Do you believe this kind of attack against connected industrial equipment will become more common?

And how many supermarkets, factories or other businesses actually know whether their OT equipment is exposed to the internet or running outdated firmware?

Wake - October 12, 2026, 2:30 pm

The s in IoT stands for security lmao, this is brilliant in my opinion.

Bastille - October 12, 2026, 2:37 pm

(Oct 12, 2026 02:30 PM)Wake Wrote: [\[CITE\]](#) The s in IoT stands for security lmao, this is brilliant in my opinion.

Hahaha, I was looking for "IoT's" in my thread then I got the joke ? crazy to see exposed devices like these on the Internet, you can find them with tools like Shodan and Censys

Unfortunately a lot of food has been wasted... I have one of these supermarket near to where I live, I'll check tomorrow to see if they've been concerned too

Wake - October 12, 2026, 2:44 pm

(Oct 12, 2026 02:37 PM)Bastille Wrote: [\[CITE\]](#) Hahaha, I was looking for "IoT's" in my thread then I got the joke ? crazy to see exposed devices like these on the Internet, you can find them with tools like Shodan and Censys

Unfortunately a lot of food has been wasted... I have one of these supermarket near to where I live, I'll check tomorrow to see if they've been concerned too

The food waste is sad but its a massive alert now to keep these systems updated or to not have them internet facing in the first place, there are going to be a lot of unplugged fridges until a patch is rolled out lmao.

Oh_Well - October 14, 2026, 11:09 pm

Hey, I didn't realize you already posted this ? Thanks for the analysis!

Bastille - October 15, 2026, 5:54 am

(Oct 14, 2026 11:09 PM)Oh_Well Wrote: [\[CITE\]](#) Hey, I didn't realize you already posted this ? Thanks for the analysis!

Haha, no worries, there are so many threads during the Octoberfest event we can definitely miss

some ?

HerrWinston - *October 16, 2026, 9:27 am*

Food loss is very unfortunate but the upside is that security might get a bit more attention now, or maybe not, thanks for this thread, always good to see something new in this section! :)

Bastille - *October 16, 2026, 9:53 am*

(26 hours ago)HerrWinston Wrote: [\[CITE\]](#) Food loss is very unfortunate but the upside is that security might get a bit more attention now, or maybe not, thanks for this thread, always good to see something new in this section! :)

Yeah companies have often been cheapskate about cyber security... I see a lot of job offer asking for a CISO doing everything from technical helpdesk to audit and incident management, alone. Maybe they'll realize this needs an entire team.

I'll do my best to post in tech and hacking sections :) I'm not fond of LQ posting during the octoberfest event, so every year I do my best to share interesting stuff haha, thanks for your post by the way :)