



**HackAtlas**

LEARNING REPORT

CASE · 2026

# Intermarché, Coopérative U en andere Franse supermarktketens

Hackers zetten koelinstallaties op 50 graden (oktober 2026)

WANNEER

**12 oktober 2026**

LAND

**Frankrijk**

SOORT AANVAL

**Sabotage**

AANVALSPAD BEKEND

**deels**

OPGESTELD DOOR

**HackAtlas.nl**

VERSIE 1

**12 oktober 2026**



Gegenereerd met behulp van AI (Claude, Anthropic). Controleer belangrijke feiten aan de hand van de bronnen in de bijlage.

# Intermarché en andere Franse supermarkten: hackers zetten koelinstallaties op 50 graden (oktober 2026)

**In het kort.** In de nacht van zondag 11 op maandag 12 oktober 2026 hebben hackers de koelinstallaties van honderden Franse supermarkten ontregeld, onder meer bij Intermarché, Coopérative U, E.Leclerc, Carrefour en Monoprix.<sup>1,2</sup> Hoe ze binnenkwamen is niet vastgesteld: het gaat om koelregelaars van het Deense bedrijf Danfoss, vooral oude of niet bijgewerkte apparaten, en volgens onze afleiding stond hun beheerpagina open naar het internet.<sup>3,4,5</sup> De aanvallers zetten de koelmeubels op ontdooien en de temperatuur tot 50 graden, waardoor vers eten en diepvries werd weggegooid, op sommige plekken brand ontstond en de schade volgens een topman in de tientallen miljoenen euro's kan lopen.<sup>1,2</sup>

**Aanvalspad deels bekend:**  5 bevestigd ·  0 gemeld ·  2 afgeleid ·  3 onbekend

Stand: maandagavond 12 oktober 2026, op basis van bronnen tot ongeveer 19.30 uur. Het onderzoek loopt nog. Wat hier "niet bekend" heet, kan later wel bekend worden.

## 1. In één oogopslag

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Organisatie    | Franse supermarktketens, vooral Intermarché en Netto (groep Les Mousquetaires) en Coopérative U (merk Système U). Ook E.Leclerc, Carrefour en Monoprix hebben last. Sector: detailhandel in Frankrijk. De getroffen regelaars komen van het Deense bedrijf Danfoss. <sup>1,3</sup>                                                                                                                                                                                                                                                                                                                                                                                    |
| Wanneer        | De nacht van zondag 11 op maandag 12 oktober 2026. In sommige winkels begon het kort na middernacht, in een winkel in Normandië rond 4.45 uur. <sup>6,7</sup> Veel winkels merkten het pas bij het openen. Het werd maandag 12 oktober bekend. <sup>8</sup>                                                                                                                                                                                                                                                                                                                                                                                                           |
| Dader          | Onbekend. In de gelezen bronnen heeft niemand de aanval opgeëist, en geen overheid noemt een dader. <sup>1,2</sup>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Soort aanval   | Sabotage van fysieke apparaten: de aanvallers veranderden de instellingen van koelregelaars. <sup>1</sup> Een losgeldeis is niet gemeld. AFP schrijft dat er geen gegevens zijn gestolen; een officiële vaststelling daarvan is niet gemeld. <sup>9</sup>                                                                                                                                                                                                                                                                                                                                                                                                             |
| Eerste toegang | Niet vastgesteld. Het CERT-FR, de alarmdienst van de Franse overheid, meldt dat veel regelaars van de series AK-SM en AK-SC zijn overgenomen. Het zegt ook dat een beheerpagina die vanaf internet bereikbaar is, niet hoort. <sup>4</sup> Wij leiden daaruit af dat de aanvallers via zo'n pagina binnenkwamen. Dat is niet bevestigd. <sup>5</sup>                                                                                                                                                                                                                                                                                                                  |
| Gevolgen       | Vers en diepgevroren eten is weggegooid in honderden winkels. Volgens de ketens zelf gaat het om ten minste 300 winkels van Intermarché en Netto, minder dan 100 van Coopérative U, 80 supermarkten van Carrefour, ongeveer 30 van Monoprix en meerdere van E.Leclerc. <sup>1</sup> Het parket van Parijs noemt ook brand. <sup>2</sup> De topman van Les Mousquetaires schat de schade voor het hele land op tientallen miljoenen euro's in één ochtend. <sup>1</sup> Intermarché zegt dat verzekeringen dit soort schade mogelijk niet dekken. <sup>9</sup> Het parket van Parijs onderzoekt de aanval en de Franse cyberdienst ANSSI is ingeschakeld. <sup>1</sup> |

## 2. Wat er gebeurde

---

**De apparaten.** Koelmeubels en koelcellen in een supermarkt hebben een regelaar die de temperatuur en de ontdooicycli beheert. Een ontdooicyclus is een korte verwarmstap die het ijs wegsmaakt.<sup>10</sup> Het Deense bedrijf Danfoss maakt zulke regelaars. Zijn systeem AK-SM 800A stuurt de regelaars van een hele winkel aan. Het heeft een webpagina voor beheer, zodat technici op afstand kunnen werken.<sup>11</sup> Koelbedrijven, frigoristen genoemd, installeren en onderhouden de installaties.<sup>12</sup> Een beheerder van een winkel in Rennes zegt dat alleen de frigorist de temperatuur kan instellen.<sup>13</sup>

**Eerdere waarschuwingen.** Op 24 maart 2025 publiceerde Danfoss een beveiligingsadvies over een fout in de AK-SM 8xxA waarmee je het inloggen kon omzeilen, met een verbeterde versie (R4.2).<sup>14</sup> De Amerikaanse overheidsdienst CISA volgde op 20 mei 2025.<sup>15</sup> Op 1 augustus 2025 kwam een advies over twee andere fouten, met versie 4.3.1.<sup>16</sup> Op 9 augustus 2026 legde het onderzoeksteam Team82 van het beveiligingsbedrijf Claroty uit hoe het werkt: een verborgen inlogcode die elke dag verandert, een fout waarmee je na het inloggen opdrachten kunt uitvoeren, en 2.765 beheerpagina's die vanaf internet bereikbaar waren.<sup>11</sup> Of een van deze fouten bij de aanval is gebruikt, is niet bekend.

**De nacht van 11 op 12 oktober.** De aanvallers veranderden in honderden winkels de instellingen van de Danfoss-regelaars. Ze zetten de koelmeubels op ontdooien en lieten de temperatuur oplopen tot 50 graden.<sup>1</sup> Volgens de VRT en andere media liep het ontdooien doorlopend door.<sup>6</sup> Een woordvoerder van Les Mousquetaires zei tegen Bloomberg dat koelmeubels ongeveer zes uur lang zo warm bleven.<sup>17</sup> Een Intermarché bij Rouen meldt dat het rond 4.45 uur gebeurde.<sup>7</sup> De beheerder van een Carrefour Market in Rennes kreeg de hele nacht alarmen, met meldingen tot 95 graden op de app. De beheerder dacht eerst aan een storing en kon zelf niets instellen.<sup>13</sup> In een winkel in Essonne kwam rook uit een koelcel.<sup>18</sup>

**Maandagochtend.** Het personeel vond ontdooide vriezers en gooide de voorraad weg.<sup>8,6</sup> In Haguenau in de Elzas verloren twee winkels samen ongeveer 270.000 euro.<sup>6</sup> De topman van Coopérative U bevestigde de aanval op X en noemde hem ongekend.<sup>1</sup> E.Leclerc zei dat een aanval een leverancier van koelapparatuur had getroffen. Les Mousquetaires zei dat Danfoss, dat de koelmeubels van de groep beheert, was aangevallen.<sup>9,3</sup> Intermarché sprak van een aanval bij een dienstverlener die koeling beheert.<sup>19</sup>

**Danfoss.** Danfoss zegt dat het om een beperkt aantal systemen gaat. De meeste zijn oud: de AK-SM800 en de AK-SC355 krijgen geen updates meer. Daarnaast draiden AK-SM800A-systemen op verouderde firmware, de ingebouwde software van het apparaat.<sup>3,20</sup> Danfoss helpt klanten met updates, strengere netwerkbeveiliging en het weghalen van directe toegang via internet.<sup>3</sup>

**De overheid.** Het parket van Parijs begon uit eigen beweging een onderzoek. De afdeling cybercriminaliteit leidt het, het Office anti-cybercriminalité (OFAC) voert het uit. Het wil de slachtoffers tellen en het verband leggen met de schade, waaronder voedselverlies en brand.<sup>1</sup> De premier vroeg ANSSI het dossier op te pakken. Een bron uit de omgeving van de premier zegt dat ANSSI al een kwetsbaarheid heeft gevonden in software van een Deens bedrijf en contact heeft opgenomen met de maker.<sup>3</sup> Volgens een bron bij ANSSI, aangehaald door Reuters, gebeurde de hack waarschijnlijk via een kwetsbaarheid in Danfoss-software.<sup>21</sup> Het CERT-FR plaatste dezelfde dag een alert met adviezen.<sup>4</sup> De brancheorganisatie FCD vroeg Danfoss en de

koelbedrijven om volledige openheid.<sup>1</sup> De Europese commissaris voor landbouw en voedsel veroordeelde de aanval.<sup>2</sup>

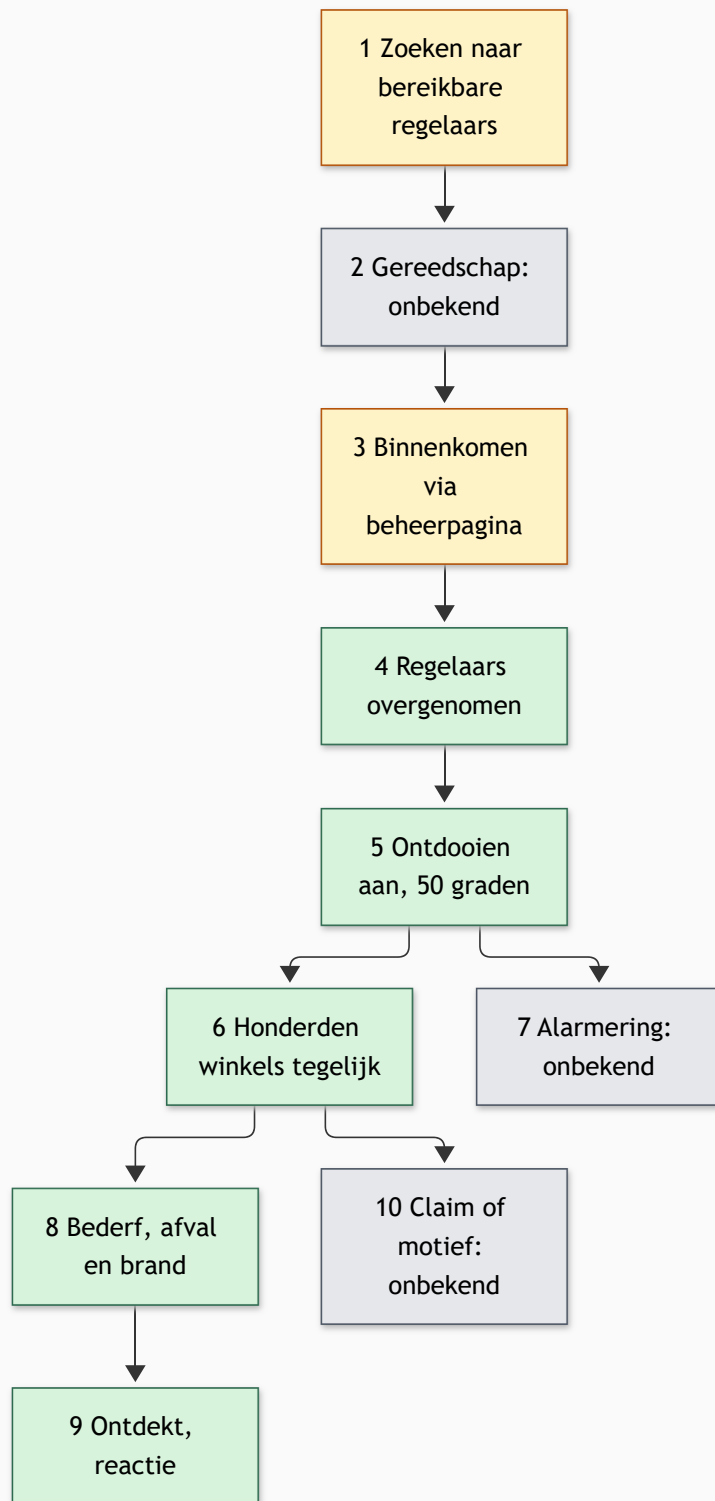
**België en Nederland.** In de kop van het AD staat dat er ook in België problemen zijn. Dat gaat over Delhaize, dat dezelfde dag een eigen storing had door het incident bij Ahold Delhaize.<sup>21</sup> De Belgische brancheorganisatie Comeos zegt dat Belgische supermarkten met Danfoss geen probleem hebben en dat het probleem bij Danfoss France zit.<sup>6</sup> Ahold Delhaize ziet geen reden voor een verband met de Franse aanval, en andere bronnen vinden daar ook geen aanwijzing voor.<sup>8,22</sup>

**Herstel.** Een Intermarché in Haguenau schreef dat het gekoelde voedsel kon worden gered dankzij snel ingrijpen van een koeltechnisch bedrijf. De diepgevroren producten moesten weg. Het diepvriesrayon wordt volgens de winkel eind van de week weer aangevuld.<sup>23</sup>

### 3. Het aanvalspad

---

Er is op maandagavond nog geen openbaar technisch rapport. Vast staat dat regelaars van Danfoss zijn overgenomen en dat hun instellingen zijn veranderd.<sup>4,1</sup> Hoe de aanvallers binnenkwamen, is niet vastgesteld. Bij elke stap staat hoe zeker we zijn.



| # | Fase (ATT&CK-tactiek)                   | Wat de aanvallers deden                                                                                                                                                     | Techniek                                                  | Zekerheid |
|---|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|-----------|
| 1 | Reconnaissance (zoeken naar doelwitten) | De aanvallers wisten waarschijnlijk welke regelaars vanaf internet bereikbaar waren. Duizenden beheerpagina's zijn te vinden met zoekmachines voor apparaten. <sup>24</sup> | <a href="#">T1596.005 Scan Databases</a> (onze koppeling) |           |

| #  | Fase (ATT&CK-tactiek)                                           | Wat de aanvallers deden                                                                                                                                                                                                 | Techniek                                                                                                                          | Zekerheid |
|----|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------|
| 2  | Resource Development en Execution (voorbereiding en uitvoering) | Welk gereedschap, welke kwetsbaarheid of welke wachtwoorden de aanvallers gebruikten, en wat ze op de regelaars deden om beheer te krijgen, is niet gemeld. <sup>4,3</sup>                                              | Techniek onbekend                                                                                                                 | ?         |
| 3  | Initial Access (binnenkomen)                                    | De aanvallers kwamen waarschijnlijk binnen via de beheerpagina die vanaf internet bereikbaar was. Media schrijven dat het via oudere versies van de software ging, maar noemen geen bron voor de route. <sup>5</sup>    | <a href="#">T1190 Exploit Public-Facing Application</a> (onze koppeling; alternatief <a href="#">T1078.001 Default Accounts</a> ) | 🗨️        |
| 4  | Initial Access (binnenkomen), uitkomst                          | Regelaars van de series AK-SM en AK-SC werden overgenomen. Het ging vooral om oude of niet bijgewerkte apparaten. <sup>4,3,20</sup>                                                                                     | Techniek: zie stap 3                                                                                                              | ✅         |
| 5  | Impact (instellingen veranderen)                                | De aanvallers zetten de koelmeubels op ontdooien en de temperatuur tot 50 graden. De topman van Les Mousquetaires zegt dat dit van afstand gebeurde. Dat het ontdooien doorlopend liep, melden media. <sup>1,17,6</sup> | <a href="#">T1565.001 Stored Data Manipulation</a> (onze koppeling <sup>25</sup> )                                                | ✅         |
| 6  | Impact (op grote schaal)                                        | In één nacht werden honderden winkels van meerdere ketens tegelijk getroffen. De ketens bevestigden de aantallen aan AFP. <sup>1</sup>                                                                                  | Geen aparte techniek (gevolg van stap 3 tot 5)                                                                                    | ✅         |
| 7  | Defense Impairment (alarmering)                                 | Of de aanvallers ook alarmen uitschakelden, is niet bekend. Eén beheerder kreeg de hele nacht alarmen. Volgens medewerkers in een vakblog ging de alarmering elders niet af. <sup>13,12</sup>                           | Techniek onbekend                                                                                                                 | ?         |
| 8  | Impact (schade)                                                 | Koelmeubels werden warm. Vers eten en diepvries werden weggegooid, en er ontstonden brand en rook. Het parket noemt voedselverlies en brand. <sup>1,2,18</sup>                                                          | Geen Enterprise-techniek; zie ATT&CK for ICS in hoofdstuk 7                                                                       | ✅         |
| 9  | Detectie en reactie                                             | Winkels merkten het door alarmen of bij het openen. Ze haalden producten weg en riepen koeltechnici. Danfoss, ANSSI en het parket reageerden. <sup>8,23,3</sup>                                                         | Geen techniek (reactie)                                                                                                           | ✅         |
| 10 | Impact (eis of claim)                                           | In de gelezen bronnen staat geen losgeldeis, claim of motief. <sup>1,2</sup>                                                                                                                                            | Techniek onbekend                                                                                                                 | ?         |

Zekerheid:  bevestigd door de organisatie, een overheid, de rechter of een onafhankelijk onderzoek ·  gemeld door betrouwbare media of onderzoekers ·  afgeleid, met de redenering in de noot ·  onbekend

## 4. Waarom het lukte

De inbraakroute is niet vastgesteld. Daarom staat bij elke oorzaak hoe zeker die is.

1. **Beheerpagina's stonden open naar het internet (✓ dat veel pagina's open staan, 🚫 dat dit de route was).** Het CERT-FR zegt dat het niet hoort en adviseert de toegang te filteren.<sup>4</sup> Danfoss wil directe toegang via internet weghalen waar dat kan.<sup>3</sup> Claroty vond in augustus 2026 2.765 bereikbare pagina's en het IT-vakblad LeMagIT telde bijna 3.000 Franse adressen.<sup>11,26</sup> Een reden: beheer op afstand scheelt reizen. Een winkelbeheerder zei dat de koeling is aangesloten zodat de frigorist storingsen op afstand ziet.<sup>18</sup>
2. **Oude apparaten, zonder updates (✓).** Volgens Danfoss zijn de meeste getroffen apparaten oud. De AK-SM800 is sinds 2021 officieel aan het einde van zijn levensduur en de AK-SC355 werd in 2016 uitgefaseerd. De AK-SM800A's draaiden op verouderde firmware.<sup>20</sup> Voor de AK-SM 800A bestonden verbeterde versies sinds maart en augustus 2025.<sup>14,16</sup> Volgens LeMagIT lijkt het merendeel van de pagina's niet na de waarschuwing van maart 2025 te zijn bijgewerkt. Een gebruikelijke reden in dit vak is dat de continuïteit voorgaat en dat men vreest dat een update iets stukmaakt.<sup>26</sup>
3. **Veel winkels hangen aan dezelfde leverancier en dezelfde beheerroute (🚫).** Winkels van meerdere ketens werden binnen enkele uren getroffen en hadden alleen Danfoss-apparatuur gemeen.<sup>13,1</sup> Medewerkers die de vakblog berichten stuurden, zeggen dat winkels die niet via het Danfoss-platform worden bewaakt, gespaard bleven. Die uitspraak is niet gecontroleerd.<sup>12</sup> Of een gedeelde beheerroute is gebruikt, is niet bekend.<sup>27</sup>
4. **Niemand was duidelijk eigenaar (🚫).** Een adviseur zegt aan AFP dat dit soort installaties is ontworpen voor betrouwbaarheid en lage kosten, niet voor bescherming tegen aanvallen op afstand.<sup>1</sup> Een vakblog schrijft dat zulke apparaten vaak door koelbedrijven worden geïnstalleerd en onderhouden en zelden door de IT-afdeling van de keten worden gevolgd.<sup>12</sup> De beheerder in Rennes kon niets zelf instellen.<sup>13</sup> Wij leiden af dat er daardoor weinig toezicht was op updates en toegang.<sup>27</sup>
5. **De schade is direct en niet terug te draaien (✓).** Zodra de koude keten breekt, moet het eten weg.<sup>9</sup> De aanval vond plaats 's nachts. In sommige winkels werd hij pas bij het openen ontdekt.<sup>8</sup> Verzekeringen dekken dit volgens Intermarché mogelijk niet.<sup>9</sup>

## 5. Wat het had kunnen stoppen

Dit zijn voorstellen op basis van de bronnen en algemene richtlijnen. Ze zijn niet getest bij de getroffen ketens. Het is niet bekend welke maatregelen zij al hadden.<sup>28</sup>

| Stap   | Maatregel                                                                                                                                                                                                                                | Moeite          | Effect                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---------------------------------------------------------------------------------------|
| 1 en 3 | Zet beheerpagina's niet op het open internet. Laat beheer alleen toe via een beveiligde verbinding (VPN) of van vaste, vertrouwde adressen. Controleer ook met een scan van eigen adressen wat van buiten te zien is. <sup>4,15,11</sup> | laag tot middel | De aanvallers konden de regelaars niet meer vinden of bereiken, als dit de route was. |

| Stap   | Maatregel                                                                                                                                                                                                                                                                                            | Moeite                               | Effect                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|------------------------------------------------------------------------------|
| 3 en 4 | Vervang apparaten waarvoor geen updates meer komen (AK-SM800, AK-SC355) en werk de firmware van de rest bij (AK-SM800A: versie 4.3.1 of nieuwer). <sup>3,11,16</sup>                                                                                                                                 | hoog (vervangen), middel (bijwerken) | Sluit bekende gaten. Danfoss zegt dit al lang te adviseren. <sup>3</sup>     |
| 5      | Bouw een tweede beveiliging in de installatie zelf, buiten het bereik van de regelaar: een eigen hoge-temperatuurbewaking die het ontdooien afkapt, en een maximale ontdooitijd die niet via het netwerk te wijzigen is. <sup>28</sup>                                                               | middel                               | Ook een overgenomen regelaar kan de koeling dan niet naar 50 graden brengen. |
| 5 en 7 | Zet een eigen, losstaande temperatuurmelding op, met een sensor en een eigen verbinding, die ook werkt als de regelaar liegt of uitvalt. <sup>28</sup>                                                                                                                                               | laag tot middel                      | Sneller ontdekken en een betrouwbaar signaal naar de beheerder.              |
| 7 en 9 | Regel dat 's nachts iemand kan ingrijpen: een koelbedrijf dat 24 uur per dag opneemt en een afspraak over wie de installatie mag loskoppelen. Een beheerder in Rennes kreeg alarmen maar kon niets doen. In Haguenau redde snel ingrijpen van een koelbedrijf het gekoelde voedsel. <sup>13,23</sup> | middel                               | Een deel van de voorraad blijft behouden.                                    |
| 9      | Zoek zelf: na de publicatie van Claroty op 9 augustus 2026 kon elke keten haar eigen apparaten opsporen en controleren. <sup>11</sup>                                                                                                                                                                | laag                                 | Er was tijd om te herstellen voor er schade was.                             |
| 8      | Leg vooraf vast wie de schade draagt (verzekering, koelbedrijf en leverancier) en of de polis dit soort schade dekt. <sup>9</sup>                                                                                                                                                                    | laag                                 | Minder onzekerheid achteraf.                                                 |

## 6. Lessen

**Voor bestuur en management** - ☐ Welke apparaten in onze winkels en gebouwen (koeling, verwarming, ventilatie, bewaking) hangen aan het internet, en wie is er verantwoordelijk voor?<sup>4,12</sup> - ☐ Welke installaties komen van leveranciers die geen updates meer leveren? Wat kost vervangen, en wat kost niets doen?<sup>20</sup> - ☐ Zijn onze verzekeringen duidelijk over schade door een aanval op machines? Intermarché noemde dit als een van de moeilijke punten.<sup>9</sup> - ☐ Wat staat er in contracten met koelbedrijven en leveranciers over updates, toegang op afstand en wie wat meldt als er iets misgaat?<sup>1</sup> - ☐ Wie mag 's nachts besluiten een installatie los te koppelen?<sup>13</sup>

**Voor IT en security** - ☐ Maak een lijst van alle apparaten met een beheerpagina en kijk met een scan van uw eigen adressen wat er van buiten te zien is.<sup>11,26</sup> - ☐ Haal beheerpagina's van het internet. Laat toegang alleen toe via een VPN of vanaf vaste adressen.<sup>4,15</sup> - ☐ Controleer de firmware van uw Danfoss-regelaars. Voor de AK-SM 800A is dat 4.3.1 of nieuwer. Maak een plan om de AK-SM800 en AK-SC355 te vervangen.<sup>11,20</sup> - ☐ Bij een vermoeden van overname: volg de stappen van het CERT-FR (toegang alleen voor de dienstverlener, fabrieksreset, alle updates, geheimen vervangen, accounts controleren, opnieuw instellen).<sup>4</sup> - ☐ Zorg voor een eigen temperatuurmelding die niet van de regelaar afhangt.<sup>28</sup> - ☐ Neem OT-apparaten (koeling, gebouwbeheer) mee in het beheer van kwetsbaarheden en volg de adviezen van fabrikanten, CISA en het CERT-FR.<sup>15,4</sup>

**Voor iedere medewerker** - ☐ Merkt u dat een koeling of vriezer te warm wordt of alarm geeft? Meld het meteen. Noteer de temperatuur en maak foto's.<sup>13</sup> - ☐ Volg de procedure van uw eigen keten bij bederf. Bij Les Mousquetaires was die: de bakken leegmaken, de schade laten vaststellen door een deurwaarder en de waren weggooien.<sup>3</sup> - ☐ Weet u waar het kastje zit dat uw koeling met internet verbindt, en wie het mag loskoppelen? Vraag het na. In één winkel koppelde de beheerder dat kastje na de aanval los.<sup>18</sup>

## 7. Voor securityprofessionals

### Technieken (MITRE ATT&CK)

Gebruikte versie: ATT&CK Enterprise v19.2 (augustus 2026) en ATT&CK for ICS v19.2. In v19 is Defense Evasion opgesplitst in Stealth (TA0005) en Defense Impairment (TA0112); [T1562](#) is vervangen door [T1685](#). Alle hieronder genoemde ID's zijn gecontroleerd in de STIX-bestanden en zijn niet ingetrokken.<sup>29</sup> Op maandagavond is er geen openbaar technisch rapport. De koppeling van feiten aan technieken is daarom van ons; de feiten zelf hebben een bron.

| Tactiek                                                                                 | Techniek                                                | Zekerheid                                                                                        | Toelichting                                                                                                                                |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Reconnaissance ( <a href="#">TA0043</a> )                                               | <a href="#">T1596.005 Scan Databases</a>                |                 | Zoeken in databases van internetscanners naar bereikbare beheerpagina's; alternatief <a href="#">T1595 Active Scanning</a> . <sup>24</sup> |
| Resource Development ( <a href="#">TA0042</a> ) en Execution ( <a href="#">TA0002</a> ) | Techniek onbekend                                       |               | Gereedschap, exploit of wachtwoorden en acties op de regelaar zijn niet gemeld. <sup>4,3</sup>                                             |
| Initial Access ( <a href="#">TA0001</a> )                                               | <a href="#">T1190 Exploit Public-Facing Application</a> |               | Webinterface van de AK-SM/AK-SC, vanaf internet bereikbaar; alternatief <a href="#">T1078.001 Default Accounts</a> . <sup>5</sup>          |
| Impact ( <a href="#">TA0040</a> )                                                       | <a href="#">T1565.001 Stored Data Manipulation</a>      |  (het effect) | Instellingen (temperatuur, ontdooien) op het apparaat veranderd. De koppeling is van ons. <sup>1,25</sup>                                  |
| Defense Impairment ( <a href="#">TA0112</a> )                                           | Techniek onbekend                                       |               | Tegenstrijdige meldingen over de alarmering. <sup>13,12</sup>                                                                              |

**ATT&CK for ICS.** Enterprise heeft geen techniek voor het aansturen van een fysiek proces. Deze ICS-technieken passen beter. Ook hier is de koppeling van ons.<sup>25,29</sup>

| Tactiek (ICS)          | Techniek                                                                                           | Zekerheid                                                                                        | Toelichting                                                       |
|------------------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Initial Access         | <a href="#">T0883 Internet Accessible Device</a>                                                   |               | Beheerpagina's bereikbaar vanaf internet. <sup>5,11</sup>         |
| Impair Process Control | <a href="#">T0836 Modify Parameter</a>                                                             |  (het effect) | Temperatuurstelling en ontdooifunctie veranderd. <sup>1</sup>     |
| Impact                 | <a href="#">T0831 Manipulation of Control</a>                                                      |  (het effect) | De koeling deed het tegenovergestelde van haar taak. <sup>1</sup> |
| Impact                 | <a href="#">T0879 Damage to Property</a> en <a href="#">T0828 Loss of Productivity and Revenue</a> |  (het effect) | Bedorven voorraad, brand en omzetverlies. <sup>1,2</sup>          |

**Hypothesen, geen bevindingen.** Er is geen bron die zegt dat een van deze technieken is gebruikt. Ze staan hier als hulp voor onderzoekers.<sup>27</sup>

| Waar               | Techniek                                                                                    | Waarom onderzoeken                                                                                                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initial Access     | <a href="#">T1078 Valid Accounts</a> , waaronder <a href="#">T1078.001 Default Accounts</a> | Het CERT-FR adviseert geheimen te vervangen en accounts te controleren, wat past bij misbruik van inloggegevens. Niets bevestigt dat. <sup>4</sup>                                                                                                   |
| Initial Access     | <a href="#">T1133 External Remote Services</a>                                              | Beheer op afstand door koelbedrijven; het CERT-FR wil toegang beperken tot de dienstverleners. <sup>4</sup>                                                                                                                                          |
| Initial Access     | <a href="#">T1199 Trusted Relationship</a>                                                  | De ketens zeggen dat een leverancier of dienstverlener is aangevallen. Een gedeelde beheerroute (een koelbedrijf of het door Danfoss gehoste platform StoreView Web) zou veel winkels tegelijk verklaren. Niets bevestigt dit. <sup>9,19,26,27</sup> |
| Execution          | <a href="#">T1059.004 Unix Shell</a>                                                        | Zou passen als <a href="#">CVE-2025-41451</a> (na inloggen) is gebruikt. <sup>11,16</sup>                                                                                                                                                            |
| Defense Impairment | <a href="#">T1685 Disable or Modify Tools</a>                                               | Zou passen als de alarmering is gemanipuleerd. <sup>12</sup>                                                                                                                                                                                         |

**Software en malware.** In de gelezen bronnen staat geen malware of hulpprogramma. De getroffen producten zijn Danfoss AK-SM 800, AK-SM 800A en AK-SC 355 en hun beheerpagina StoreView.<sup>3,11</sup>

**Kwetsbaarheden**

Geen bron zegt dat een van deze kwetsbaarheden bij de aanval is gebruikt. Ze staan hier omdat ze dezelfde apparaten betreffen en omdat Danfoss zegt dat AK-SM800A-systemen verouderde firmware draaiden.<sup>20</sup> Ze staan niet in het veld `cves` van deze case.

| CVE                            | Product                                                                                                         | Ernst (CVSS)                       | Actief misbruikt (CISA KEV)                                | Patch beschikbaar sinds               | Misbruik vanaf           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------------------------------|---------------------------------------|--------------------------|
| <a href="#">CVE-2025-41450</a> | Danfoss AK-SM 8xxA vóór R4.2: verborgen dagcode die inloggen omzeilt <sup>11,14</sup>                           | 8,2 (v3.1), 7,3 (v4) <sup>15</sup> | Nee, niet in de catalogus van 8 oktober 2026 <sup>30</sup> | 24 maart 2025 (R4.2) <sup>14</sup>    | Onbekend; niet bevestigd |
| <a href="#">CVE-2025-41451</a> | Danfoss AK-SM 8xxA vóór 4.3.1: opdrachten invoegen via alarm-naar-mail-velden, na inloggen <sup>16</sup>        | 7,6 (v3.1), 8,7 (v4) <sup>15</sup> | Nee, niet in de catalogus van 8 oktober 2026 <sup>30</sup> | 1 augustus 2025 (4.3.1) <sup>16</sup> | Onbekend; niet bevestigd |
| <a href="#">CVE-2025-41452</a> | Danfoss AK-SM 8xxA vóór 4.3.1: nginx-instellingen invoegen, na inloggen; het beheer kan uitvallen <sup>16</sup> | 5,4 (v3.1), 6,8 (v4) <sup>15</sup> | Nee, niet in de catalogus van 8 oktober 2026 <sup>30</sup> | 1 augustus 2025 (4.3.1) <sup>16</sup> | Onbekend; niet bevestigd |

CISA schreef bij de laatste herziening in augustus 2025 dat het geen bekend openbaar misbruik van deze fouten had gezien.<sup>15</sup> Oudere firmware heeft ook andere fouten: voor de AK-SM 800A vóór versie 3.3 gaf Danfoss in augustus 2023 een advies met [CVE-2023-25913](#), [CVE-2023-25914](#) en [CVE-2023-25915](#), de laatste een externe uitvoering van opdrachten met CVSS 9,8.<sup>31</sup> Voor AK-SM800 en AK-SC355 komen geen updates meer.<sup>3</sup>

De Danfoss-waarschuwing die AFP (met de datum 18 september) en Tweakers (met de maand augustus) noemen, over het lezen en schrijven van interne waarden en het uploaden van niet-ondertekende programma's, komt overeen met advies DSA-2026-08-01 ([CVE-2026-15203](#), CVSS 9,3). Dat gaat over iC7-software voor aandrijvingen; AK-SM- en AK-SC-regelaars staan er niet bij. Wij leggen geen verband. <sup>1,32,33,34</sup>

## Sporen van de aanvallers

Er zijn geen IP-adressen, domeinen, bestandshashes of vermeldingen op een leksite openbaar gedeeld in de gelezen bronnen. <sup>4,19</sup> Wat wel openbaar is, zijn tellingen van bereikbare beheerpagina's: 2.765 AK-SM 800A volgens een telling van Claroty met Censys, 2.752 Danfoss-systemen waarvan 1.590 in Frankrijk volgens een onderzoeker van Predicta Lab, en bijna 3.000 Franse adressen volgens LeMagIT. <sup>11,19,26</sup> De methoden verschillen en de cijfers zijn niet gelijk te stellen. Veel apparaten tonen de HTTP-titel van de Danfoss StoreView-beheerpagina. <sup>11</sup>

## Detectie en respons

**Wat het CERT-FR adviseert.** Alleen toegang voor de dienstverlener laten bestaan, een fabrieksreset uitvoeren, alle beschikbare updates installeren, geheimen vervangen, bestaande accounts controleren en het apparaat volledig opnieuw instellen. Eerste tijdelijke maatregel: toegang beperken tot vertrouwde IP-adressen. <sup>4</sup>

**Voorstellen (geen bevindingen).** - Maak vóór de fabrieksreset een kopie van de configuratie en de logboeken van het apparaat, voor onderzoek en voor de verzekeraar. Een reset wist ook de sporen. <sup>28</sup> - Controleer per regelaar de laatste wijzigingen in temperatuurinstellingen, ontdooischema's, gebruikers en de e-mailinstellingen voor alarmen. Dat laatste veld wordt in [CVE-2025-41451](#) genoemd. <sup>16,28</sup> - Vergelijk de gelogde temperaturen van de regelaar met een onafhankelijke sensor. Een verschil wijst op manipulatie. <sup>28</sup> - Zoek met een scan van uw eigen adresruimte naar bereikbare StoreView-pagina's en zet ze achter een VPN. <sup>11,26</sup> - Leg vast wat er op locatie is gebeurd: temperaturen, foto's en de vaststelling door een deurwaarder, zoals de procedure bij Les Mousquetaires voorschrijft. <sup>3</sup> - Houd alle meldingen over uw Danfoss-apparaten in de gaten bij CISA, Danfoss en het CERT-FR. Het onderzoek van het parket en van ANSSI kan nog nieuwe feiten brengen. <sup>1,15,4</sup>

## 8. Wat we niet weten

- **Hoe kwamen de aanvallers binnen?** Geen bron noemt de route. NOS en AD schrijven dat ze via oudere versies van de software binnenkwamen. AFP en Danfoss zeggen alleen dat de getroffen apparaten oud of niet bijgewerkt waren, en het CERT-FR noemt geen route. <sup>8,21,1,4</sup> Een rapport van ANSSI, het parket of Danfoss kan dit beantwoorden.
- **Was het een bekende kwetsbaarheid, een standaardwachtwoord of iets anders?** Een bron bij ANSSI noemt volgens Reuters een kwetsbaarheid in Danfoss-software, zonder naam. <sup>21</sup> Geen bron koppelt de aanval aan een CVE. <sup>19,22</sup>
- **Was het een aanval op de apparaten zelf of op een leverancier of dienstverlener?** E.Leclerc en Les Mousquetaires zeggen dat een leverancier is aangevallen, en Intermarché noemt een dienstverlener.

Danfoss en het CERT-FR spreken van overgenomen apparaten met een open beheerpagina.<sup>9,3,19,4</sup> Comeos plaatst het probleem bij Danfoss France.<sup>6</sup> Dit blijft open.

- **Wie zit erachter en waarom?** Er is geen claim en geen toeschrijving.<sup>1,2</sup> AFP zet de aanval neer tegen de achtergrond van zorgen over Russische hybride aanvallen, maar dat is context, geen bewijs.<sup>35</sup>
- **Hoeveel winkels zijn getroffen?** De aantallen lopen uiteen. De ketens bevestigden aan AFP ten minste 300 Intermarché en Netto, minder dan 100 Coopérative U, 80 Carrefour, ongeveer 30 Monoprix en meerdere E.Leclerc.<sup>1</sup> Eerdere berichten noemden 150 tot 200 Intermarché en bijna 100 Coopérative U.<sup>35</sup> Bloomberg meldde ongeveer 150 Intermarché.<sup>17</sup> BleepingComputer meldt dat Franse media 250 tot 350 winkels noemen, en Cooling Post schat ongeveer 500.<sup>19,20</sup> Een totaal staat niet vast.
- **Hoe groot is de schade?** De topman van Les Mousquetaires noemt tientallen miljoenen euro's voor het hele land.<sup>1</sup> Per winkel lopen de bedragen van ongeveer 10.000 euro in een kleine winkel tot ongeveer 270.000 euro voor twee winkels in Haguenau.<sup>13,6</sup> Wie de schade betaalt (verzekering, koelbedrijf of Danfoss), is niet bekend.<sup>9</sup>
- **Werd de alarmering uitgeschakeld?** Een beheerder in Rennes kreeg de hele nacht alarmen. Medewerkers in een vakblog zeggen dat het alarm elders niet afging. Die uitspraken zijn niet gecontroleerd.<sup>13,12</sup>
- **Welke versies zijn getroffen?** Danfoss noemt AK-SM800, AK-SC355 en AK-SM800A met verouderde firmware. BFMTV, aangehaald door anderen, zegt dat het gaat om versies vóór 4.<sup>3,23</sup> Welke versie in welke winkel draaide, is niet bekend.
- **Werden gegevens gestolen?** AFP schrijft van niet, maar een onderzoeksuitkomst is er niet.<sup>9</sup>
- **Waarom werden sommige winkels gespaard?** Medewerkers in een vakblog zeggen dat winkels die via het Danfoss-platform worden bewaakt, werden getroffen. Dat is niet gecontroleerd.<sup>12</sup>
- **Is er een verband met de storingen bij Amerikaanse militaire winkels in augustus 2026?** Daar vielen koelingen uit; militaire opsporingsdiensten onderzoeken dat en er is geen oorzaak gepubliceerd. De dienst zegt dat uitval in vier Europese winkels daar los van staat.<sup>36,37</sup> Geen gelezen bron legt een verband met Frankrijk.<sup>22</sup>
- **Is er een verband met Ahold Delhaize?** Ahold Delhaize ziet geen reden daarvoor, en HNS ziet geen aanwijzing.<sup>8,22</sup>
- **Is het onderzoek van Claroty ook op DEF CON (een hackerconferentie) gepresenteerd?** Franse media zeggen van wel. De gelezen Claroty-pagina noemt dat niet.<sup>11,23</sup> Dat verandert niets aan de inhoud.
- **Is er al een uitkomst van het onderzoek?** In de gelezen bronnen hebben het parket en ANSSI nog niets gepubliceerd over de toedracht.<sup>1,3</sup>

## 9. Begrippen

---

**Aanvalspad:** de stappen die aanvallers zetten, van binnenkomen tot de schade.

**ANSSI:** de Franse overheidsdienst voor digitale veiligheid. Het CERT-FR is het onderdeel dat waarschuwt en adviseert.<sup>4</sup>

**Beheerpagina:** een webpagina waarmee je een apparaat instelt. Staat die open naar het internet, dan kan in principe iedereen proberen er in te komen.

**CVE:** een vast nummer voor een bekende fout in software of een apparaat.

**CVSS:** een score van 0 tot 10 voor hoe ernstig een kwetsbaarheid is.

**Firmware:** de ingebouwde software van een apparaat, zoals van een koelregelaar.

**Frigorist:** een koelbedrijf dat koelinstallaties plaatst en onderhoudt.

**Koude keten:** de reeks waarin eten steeds koud blijft, van fabriek tot winkelschap. Als de temperatuur te hoog wordt, moet het eten weg.

**Ontdooicyclus:** een korte, geplande verwarmstap waarbij het ijs van een koeling smelt. Bij de aanval liet de aanvalleur de koeling veel te lang verwarmen.<sup>10</sup>

**OT (operationele technologie):** computers die machines en installaties aansturen, zoals koeling, in plaats van kantoorcomputers.

**Parket:** het openbaar ministerie in Frankrijk, dat strafzaken onderzoekt en vervolgt.

**Regelaar:** het apparaat dat de temperatuur van een koelmeubel of koelcel bepaalt.

**Sabotage:** opzettelijk iets kapotmaken of laten falen, hier met instellingen op afstand.

**Vaststelling door een deurwaarder (huissier):** een officiële vaststelling van de schade door een deurwaarder, wat de procedure bij Les Mousquetaires voorschrijft.<sup>3</sup>

**VPN:** een beveiligde verbinding via internet, waarmee alleen bekende gebruikers bij een systeem kunnen.

## Versies

---

- v1 (2026-10-12): eerste versie, op basis van bronnen tot maandagavond 12 oktober 2026.

## Bijlage: bronnen en noten

---

1. Agence France-Presse. (2026, 12 oktober). Des supermarchés français touchés par une cyberattaque inédite de leurs installations frigorifiques. *Boursorama*. <https://www.boursorama.com/bourse/actualites/des-supermarches-francais-touches-par-une-cyberattaque-inedite-de-leurs-installations-frigorifiques-d53950f3510078125e9f4b571d62aa19> (Bijgewerkte AFP-versie. Bevat de aantallen die de winkelketens aan AFP bevestigden, het bericht van het parket, de verklaring van Danfoss en uitspraken van de topman van Les Mousquetaires op BFMTV. BFMTV zelf is niet geopend.)
2. Agence France-Presse. (2026, 12 oktober). Hackers turn up the heat in refrigerators at hundreds of supermarkets in France, sparking fires and food losses. *CBS News*. <https://www.cbsnews.com/news/cyberattack-supermarkets-refrigerators-france-fires-food-losses/> (AFP-bericht, met een aanvulling van Reuters over Carrefour.)
3. franceinfo. (2026, 12 oktober). Des magasins Système U, Intermarché, E.Leclerc et Monoprix touchés par une cyberattaque contre leurs installations frigorifiques. *franceinfo*. [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/des-magasins-systeme-u-et-intermarche-touches-par-une-cyberattaque-contre-leurs-installations-frigorifiques\\_8233720.html](https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/des-magasins-systeme-u-et-intermarche-touches-par-une-cyberattaque-contre-leurs-installations-frigorifiques_8233720.html) (Gepubliceerd 12.03 uur, bijgewerkt 16.28 uur. Bevat de verklaringen van Les Mousquetaires, E.Leclerc en Danfoss en de mededeling uit de omgeving van de premier over ANSSI.)
4. CERT-FR. (2026, 12 oktober). Incident de sécurité ciblant les Danfoss série AK-SM et AK-SC (CERTFR-2026-ALE-012) [Alertebericht]. Agence nationale de la sécurité des systèmes d'information. <https://www.cert.ssi.gouv.fr/alerte/CERTFR-2026-ALE-012/> (Eerste en enige versie van 12 oktober 2026. Het bericht noemt geen aanvalsroute, geen kwetsbaarheid en geen dader.)

5. Afgeleid (binnenkomen via een beheerpagina die vanaf internet bereikbaar is). Redenering: (1) het CERT-FR meldt overnames van de series AK-SM en AK-SC, noemt een beheerpagina op internet in strijd met de goede praktijk en zet als eerste maatregel het filteren van toegang (zie noot 4); (2) Danfoss wil bij klanten waar nodig de directe verbinding met internet weghalen (zie noot 3); (3) de apparaten hebben een webpagina voor beheer en duizenden daarvan zijn bereikbaar (zie noot 11 en noot 26); (4) NOS en AD schrijven dat de hackers via oudere versies van de software binnenkwamen, zonder bron voor de route (zie noot 8 en noot 21). Alternatieven zijn standaard- of gestolen wachtwoorden, een gedeelde route via een koelbedrijf of het door Danfoss gehoste platform, of een fout die Danfoss al kent (zie hoofdstuk 7). Niets hiervan is bevestigd. T1190 is onze koppeling; T1078.001 is het belangrijkste alternatief.
6. Smits, E. (2026, 12 oktober). Cyberaanval doet koelinstallaties van supermarkten in Frankrijk op hol slaan, België niet getroffen. *VRT NWS*. <https://www.vrt.be/vrtnws/nl/2026/10/12/cyberaanval-treft-koelinstallaties-van-supermarkten-in-frankrijk/> (Gelezen via Google Nieuws. Bevat de verklaring van de Belgische brancheorganisatie Comeos.)
7. Prigent, I. (2026, 12 oktober). Cyberattaque sur les frigos : plusieurs magasins Intermarché et Carrefour Market de Seine-Maritime et de l'Eure touchés. *ICI Normandie (Radio France)*. <https://www.ici.fr/normandie/seine-maritime-76/grand-couronne/cyberattaque-sur-les-frigos-l-intermarche-de-grand-couronne-jette-tous-ses-produits-frais-et-surgeles-1495694> (Gepubliceerd 12.51 uur. Het tijdstip komt van de winkel in Grand-Couronne zelf.)
8. Agence France-Presse. (2026, 12 oktober). Cyberaanval treft Franse supermarkten, koelsystemen op 50 graden gezet. *NOS Nieuws*. <https://nos.nl/artikel/2634691-cyberaanval-treft-franse-supermarkten-koelsystemen-op-50-graden-gezet> (Gepubliceerd 15.20 uur, aangepast 18.55 uur. Zegt dat de hackers via verouderde software binnenkwamen, zonder bron voor die route.)
9. Agence France-Presse. (2026, 12 oktober). Cyberattaque inédite en France: Supermarchés contraints de jeter des produits frais. *20 minutes*. <https://www.20min.ch/fr/story/en-france-une-vaste-cyberattaque-touche-des-supermarches-103648654> (Eerdere AFP-versie. De openingszin zegt dat er geen gegevens zijn gestolen; als bewering van AFP, niet als onderzoeksuitkomst. Bevat de verklaringen van E.Leclerc en Intermarché.)
10. Waqas. (2026, 12 oktober). Hackers heat supermarket fridges to 50°C in France cyberattack. *Hackread*. <https://hackread.com/hackers-heat-supermarket-fridges-50c-france-cyberattack/> (Legt uit wat een ontdooicyclus is en noemt BFMTV, Clubic, 01net en Capital als bronnen; die zijn niet geopend.)
11. Zaltzman, A. (2026, 9 augustus). *Freeze the controller, defrost the food: Uncovering vulnerabilities in Danfoss refrigeration controllers* [Blogbericht]. Claroty Team82. <https://claroty.com/team82/research/freeze-the-controller-defrost-the-food-uncovering-vulnerabilities-in-danfoss-refrigeration-controllers> (Beschrijft de AK-SM 800A. De pagina zegt niet dat het onderzoek op DEF CON is gepresenteerd.)
12. Le Borgne, J. (2026, 12 oktober). Une cyberattaque coupe le froid dans plusieurs supermarchés (Intermarché, U, Market, Monoprix, Leclerc concernés). *Je Bosse en Grande Distribution*. <https://www.jebosseengrandedistribution.fr/2026/10/12/intermarche-u-market-monoprix-leclerc-une-cyberattaque-coupe-le-froid-dans-les-supermarches/> (Vakblog. Veel uitspraken komen van anonieme medewerkers die de site berichten stuurden; de auteur zegt zelf dat de cijfers voorzichtig moeten worden gelezen. Het is dus geen bevestiging.)
13. Peigné, T. (2026, 12 oktober). « J'ai eu des alarmes toute la nuit, certaines indiquaient des sondes à 95 °C » : coup dur pour ce supermarché victime de la cyberattaque des frigos. *France 3 Bretagne*. <https://france3-regions.franceinfo.fr/bretagne/ille-et-vilaine/rennes/j-ai-eu-des-alarmes-toute-la-nuit-certaines-indiquaient-des-sondes-a-95-c-coup-dur-pour-ce-supermarche-victime-de-la-cyberattaque-des-frigos-3432327.html> (Gepubliceerd 18.43 uur. Getuigenis van de beheerder van een Carrefour Market in Rennes; de uitspraken van de beheerder zijn niet gecontroleerd.)
14. Danfoss. (2025, 24 maart). *DSA-2025-03-01: Improper Authentication vulnerability in Danfoss AK-SM8xxA Series, resulting in an authentication bypass* [Beveiligingsadvies]. <https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/dsa-2025-03-01/> (Bijgewerkt op 1 september 2025 voor het zwakteidstype.)
15. Cybersecurity and Infrastructure Security Agency. (2025, 20 mei; bijgewerkt 26 augustus 2025). *Danfoss AK-SM 8xxA Series (Update A)* (ICSA-25-140-03) [ICS-advies]. CISA. <https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03> (De scores staan in het advies. CISA schreef dat er geen bekend openbaar misbruik was gemeld.)
16. Danfoss. (2025, 1 augustus). *DSA-2025-08-01: Post-authentication vulnerabilities, OS command injection RCE and Nginx configuration injection in Danfoss AK-SM8xxA Series* [Beveiligingsadvies]. <https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/dsa-2025-08-01/>
17. Popa, D. (2026, 12 oktober). Hackers defrost fridges at hundreds of French supermarkets, Bloomberg says. *The Next Web*. <https://thenextweb.com/news/french-supermarket-refrigeration-cyberattack-intermarche> (Geeft het bericht van Bloomberg weer; Bloomberg zelf is niet geopend.)
18. franceinfo. (2026, 12 oktober). TÉMOIGNAGE. « On a tout jeté » : une gérante d'un magasin raconte son désarroi après la cyberattaque qui a touché ses installations frigorifiques. *franceinfo*. [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/temoignage-on-a-tout-jete-une-gerante-d-un-magasin-raconte-son-desarroi-apres-la-cyberattaque-qui-a-touche-ses-installations-frigorifiques\\_8234230.html](https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/temoignage-on-a-tout-jete-une-gerante-d-un-magasin-raconte-son-desarroi-apres-la-cyberattaque-qui-a-touche-ses-installations-frigorifiques_8234230.html) (Gepubliceerd 19.24 uur. Getuigenis van een winkelbeheerder in Étréchy; de uitspraken van de beheerder zijn niet gecontroleerd.)
19. Gatlan, S. (2026, 12 oktober). Cyberattack shuts down refrigerators at French supermarkets. *BleepingComputer*. <https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-refrigerators-at-french-supermarkets/> (Bijgewerkt met de verklaring van Intermarché. Noemt de telling van een onderzoeker van Predicta Lab van 2.752 bereikbare Danfoss-systemen, waarvan 1.590 in Frankrijk; die post zelf is niet geopend.)

20. Cooling Post. (2026, 12 oktober). Danfoss moves to mitigate cyberattack. *Cooling Post*. <https://www.coolingpost.com/world-news/danfoss-moves-to-mitigate-cyberattack/> (Bevat een verklaring van Danfoss aan het vakblad en de schatting van ongeveer 500 winkels; het blad zegt dat het exacte aantal niet bekend is.)
21. Buitenlandredactie. (2026, 12 oktober). Hackers laten koelinstallaties van Franse supermarkten op hol slaan, ook in België problemen. *AD*. <https://www.ad.nl/buitenland/hackers-laten-koelinstallaties-van-franse-supermarkten-op-hol-slaan-ook-in-belgie-problemen~aa9df1fb/> (Gepubliceerd 14.11 uur, laatste update 19.10 uur. Gelezen via Google Nieuws. De problemen in België in de kop gaan over Delhaize. Het bericht van Reuters over ANSSI is niet geopend.)
22. Zorz, Z. (2026, 12 oktober). Cyberattacks hit European grocers: French supermarket freezers hijacked, Dutch and Belgian stores disrupted. *Help Net Security*. <https://www.helpnetsecurity.com/2026/10/12/france-cyberattack-supermarket-freezers/>
23. C.B. (2026, 12 oktober). Cyberattaque sur les systèmes frigorifiques de plusieurs enseignes. *Points de Vente*. <https://pointsdevente.fr/fil-info/2026-10-12-cyberattaque-sur-les-systemes-frigorifiques-de-plusieurs-enseignes/> (Vakblad. Citeert BFMTV, berichten op X van een verslaggever van BFMTV en van de hoofdredacteur van LeMagIT, en een Facebookbericht van een Intermarché in Haguenau; die zijn niet geopend.)
24. Afgeleid (zoeken naar bereikbare regelaars). Redenering: (1) de aanvallers troffen in enkele uren honderden apparaten bij meerdere ketens, wat een lijst met bereikbare doelwitten vooraf veronderstelt (zie noot 1 en noot 2); (2) Claroty vond met de zoekmachines voor apparaten Shodan en Censys 2.765 bereikbare AK-SM 800A-beheerpagina's (zie noot 11) en LeMagIT telde bijna 3.000 Franse adressen met een Danfoss-beheerpagina (zie noot 26); (3) een adviseur zegt dat een aanval op honderden apparaten tegelijk een zekere verfijning toont (zie noot 1). Dit bewijst niet hoe de aanvallers hun doelwitten vonden, en geen bron zegt dat ze zulke zoekmachines gebruikten. De techniek is onze koppeling.
25. Techniekeuze voor de stappen 5 en 8. ATT&CK Enterprise heeft geen techniek voor het sturen van een fysiek proces. Wij koppelen daarom aan [T1565.001](#) Stored Data Manipulation (instellingen op het apparaat veranderen) en noemen in hoofdstuk 7 de beter passende technieken uit ATT&CK for ICS. MITRE koppelt dit incident zelf niet. De ID's zijn gecontroleerd in versie 19.2 (zie noot 29). [T0855](#) Unauthorized Command Message is in ATT&CK for ICS ingetrokken en daarom niet gebruikt.
26. Rieß-Marchive, V. (2026, 12 oktober). Cyberattaque Danfoss : quand la distribution alimentaire découvre l'hygiène numérique. *LeMagIT*. <https://www.lemagit.fr/actualites/366652072/Cyberattaque-Danfoss-quand-la-distribution-alimentaire-decouvre-lhygiene-numerique> (Analyse van de hoofdredacteur. De telling van bereikbare pagina's is de eigen telling van de auteur; de methode is niet beschreven.)
27. Deze lijst, de uitspraak over een gedeelde beheerroute en de uitspraak over weinig toezicht zijn geen reconstructie. Redenering: (1) de ketens spreken van een aanval bij een leverancier of dienstverlener (zie noot 9, noot 3 en noot 19), terwijl Danfoss en het CERT-FR over overgenomen apparaten spreken (zie noot 3 en noot 4); (2) winkels van meerdere ketens met dezelfde leverancier werden binnen enkele uren getroffen (zie noot 1 en noot 13); (3) LeMagIT beschrijft StoreView Web, een door Danfoss gehost platform waarmee apparaten worden beheerd (zie noot 26); (4) een vakblog en een adviseur beschrijven dat zulke apparatuur door koelbedrijven wordt beheerd en slecht is beschermd (zie noot 12 en noot 1); (5) het CERT-FR vraagt geheimen te vervangen en accounts te controleren (zie noot 4); (6) [CVE-2025-41451](#) volgt uit het onderzoek van Claroty en het advies van Danfoss (zie noot 11 en noot 16). Geen bron bevestigt een van deze mogelijkheden. De technieken zijn gecontroleerd in ATT&CK v19.2 (zie noot 29).
28. Voorstel van de schrijver van deze case, gebaseerd op de adviezen van het CERT-FR, CISA en Claroty (zie noot 4, noot 15 en noot 11) en op de verhalen van de winkels (zie noot 13 en noot 23). Geen bron bevestigt dat deze maatregelen de aanval hadden gestopt, en niet bekend is welke maatregelen de ketens al hadden. De eigen hoge-temperatuurbeveiliging, de maximale ontdooitijd, de losstaande temperatuurmelding en de kopie vóór de reset zijn algemene ideeën van de schrijver; ze komen niet uit een van de bronnen.
29. MITRE. (2026, 5 augustus). *Enterprise ATT&CK en ATT&CK for ICS, release 19.2* [Gegevensbestanden]. GitHub, mitre-attack/attack-stix-data. <https://raw.githubusercontent.com/mitre-attack/attack-stix-data/master/enterprise-attack/enterprise-attack.json> (Gebruikt om te controleren dat de genoemde ID's bestaan en niet zijn ingetrokken. Het ICS-bestand staat op dezelfde plek onder ics-attack.)
30. Cybersecurity and Infrastructure Security Agency. (2026, 8 oktober). *Known Exploited Vulnerabilities Catalog* (catalogusversie 2026.10.08, 1.739 vermeldingen) [Gegevensbestand]. CISA. [https://www.cisa.gov/sites/default/files/feeds/known\\_exploited\\_vulnerabilities.json](https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json) (Op 12 oktober 2026 gecontroleerd: de drie CVE's van 2025 en de drie van 2023 staan er niet in. De catalogus kan na de aanval nog worden aangevuld.)
31. Danfoss. (2023, 21 augustus). *DSA-2023-08-01: Insufficient restrictions and input sanitization exist in Danfoss AK-SM 800A, potentially leading to full system compromise* [Beveiligingsadvies]. <https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/dsa-2023-08-01/>
32. Himmelbauer, I. (2026, 12 oktober). Koelingen van Franse supermarkten ontdooien door cyberaanval. *Tweakers*. <https://tweakers.net/nieuws/253220/koelingen-van-franse-supermarkten-ontdooien-door-cyberaanval.html> (Gepubliceerd 15.27 uur. Noemt de topman van Coopérative U ten onrechte de ceo van Intermarché en beschrijft een Danfoss-waarschuwing die volgens de Danfoss-lijst een ander product betreft (zie noot 33).)
33. Danfoss. (2026, 18 september). *DSA-2026-08-01: Debug interfaces are accessible by default in Danfoss iC7 Automation SP, iC7 Marine and iC7 Hybrid software* [Beveiligingsadvies]. <https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/dsa-2026-08-01/> (Datum is die van de laatste wijziging volgens de lijst met adviezen, zie noot 34.)

34. Danfoss. (z.d.). *Danfoss security advisories* [Webpagina]. <https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/> (Geraadpleegd op 12 oktober 2026. De lijst voor 2026 bevat alleen DSA-2026-08-01, over iC7-software. AK-SM- en AK-SC-regelaars staan daar niet bij.)
35. Paponaud, E. (2026, 12 oktober). Hundreds of French supermarkets hit by cyberattack on refrigeration systems. *Euronews*. <https://www.euronews.com/2026/10/12/hundreds-of-french-supermarkets-hit-by-cyberattack-on-refrigeration-systems> (Gepubliceerd 16.19 uur. Gebaseerd op AFP; noemt de eerdere aantallen en de zorgen over Russische hybride aanvallen.)
36. Seck, H. H. (2026, 28 augustus). DoD confirms 'refrigeration disruption' at military commissaries. *Military Times*. <https://militarytimes.com/news/your-military/2026/08/28/dod-confirms-refrigeration-disruption-at-military-commissaries/>
37. Svan, J. H. (2026, 30 september). Refrigeration failures affect 4 military commissaries in Europe. *Stars and Stripes*. <https://www.stripes.com/theaters/europe/2026-09-30/freezer-outages-europe-commissaries-23013166.html>