VORFALL-LAGEBILD

Angriff über einen Kältedienstleister trifft Kühlräume des französischen Blutspendedienstes EFS

Stand 08.11.2026 10:50 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Beim EFS hat die unabhängige Alarmierung samt Nachtbereitschaft den Schaden verhindert, das ist gelebte ICS Incident Response (CC1) und sollte jeder Betreiber von Kühlräumen im Gesundheitswesen haben.

2. Der Weg ging über den Fernzugang eines Dienstleisters, deshalb gehört jeder Wartungszugang vom Internet weg, hinter VPN mit Mehrfaktor-Anmeldung und zeitlich begrenzt freigeschaltet (CC4 Secure Remote Access).

3. Wer seine vernetzten Kältesteuerungen und deren Fernzugänge nicht kennt, kann sie nicht schützen: Asset-Inventar, Patch-Stand und Austauschplan für End-of-Life-Geräte (CC5) sind mit KI-Unterstützung auch für kleine Teams in Tagen machbar.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Das EFS meldet einen „incident de cybersécurité“ bei einem „prestataire d'équipements frigorifiques“. Betroffen waren Systeme zur Überwachung und Steuerung von Kühlräumen an drei EFS-Standorten.	100 %	100 %	bestätigt
Laut EFS wurden Temperatur- und Abtauschwellen „auf sehr hohe Temperaturen“ gesetzt. Das EFS nennt keine Gradzahl.	100 %	100 %	bestätigt
Le Canard enchaîné berichtet von einem Sollwert von 110 °C statt minus 30 °C und nennt den Dienstleister Coolworld. AFP übernimmt beides als Angabe des Canard.	100 %	100 %	bestätigt
Coolworld spricht von einer Schwachstelle in einer Komponente eines Drittanbieters und von einer „begrenzten Zahl“ betroffener Geräte. Angegriffen wurde laut AFP eine Software zur Fernüberwachung der Kühlsysteme.	100 %	100 %	bestätigt
Einer der drei Standorte ist laut France 3 Bois-Guillaume (Seine-Maritime). Laut Canard und AFP liegt mindestens einer in Bourgogne-Franche-Comté.	100 %	60 %	offen
Der Zugang lief über eine aus dem Internet erreichbare Fernwartungs- oder Überwachungsoberfläche des Dienstleisters.	70 %	70 %	offen
Der Vorfall gehört zur selben Angriffswelle wie die Supermarkt-Fälle.	50 %	55 %	offen
Gezielte staatliche Sabotage am Gesundheitswesen	15 %	12 %	offen

Frühere Aussage	vorher	jetzt	Status
Laut EFS gibt es keine gesundheitlichen Folgen und keinen Verlust von Blutprodukten. Der Vorfall sei rasch unter Kontrolle gewesen, „sans impact sur les produits et échantillons“.	100 %	100 %	bestätigt
Betroffen waren Plasmabeutel für Transfusionen und Plasma für die Arzneimittelherstellung (Fraktionierung). Anfangs hatte das EFS nur von Spenderproben gesprochen.	100 %	100 %	bestätigt
Die Produkte wurden vorsorglich in andere Anlagen verlegt, Fernzugriffe gesperrt und die Überwachung verstärkt.	100 %	95 %	präzisiert
Das EFS hat eigene Überwachungssysteme, die vom Kühlanlagenbauer unabhängig sind. Alarme und Verfahren haben die schnelle Reaktion möglich gemacht.	100 %	90 %	präzisiert
Die Versorgung von Patienten mit Blutprodukten war nicht beeinträchtigt.	85 %	88 %	offen
Ohne die unabhängige Temperaturüberwachung wäre Plasma verloren gegangen.	60 %	60 %	offen
Das Gesundheitsministerium (Ministerin Stéphanie Rist) sagt, die technischen Untersuchungen zu Vorgehen, Umfang und Wiederinbetriebnahme laufen noch.	100 %	100 %	bestätigt
Laut EFS wurden die betroffenen Geräte „maîtrisés“ oder „neutralisés“. Das EFS arbeitet mit der ANSSI und dem Ministerium zusammen.	100 %	100 %	bestätigt
CERT-FR schreibt bei den Supermarkt-Fällen, dass ein Werksreset allein nicht reicht. Er entfernt eine eingenistete Schadsoftware, das Gerät bleibt aber angreifbar.	100 %	100 %	bestätigt
Die Kühlung selbst läuft lokal weiter, offline bleibt vor allem der Fernzugang.	70 %	72 %	offen
Bis der Fernzugang sauber wieder aufgebaut ist (VPN, neue Zugangsdaten, Patch oder neue Hardware), dauert es Wochen.	45 %	45 %	offen
Laut EFS ist kein Produkt verloren gegangen oder verändert worden.	100 %	100 %	bestätigt
Verändert wurden laut Berichten Sollwerte und Schwellen in der Steuerung. Mechanische Schäden werden nicht gemeldet.	100 %	100 %	bestätigt
Mechanisch ist nichts Dauerhaftes kaputt, es wurde vor allem die Konfiguration verändert.	65 %	68 %	offen
Einzelne Steuergeräte oder Komponenten werden ausgetauscht, statt sie nur zu patchen.	35 %	35 %	offen

Frühere Aussage	vorher	jetzt	Status
CERT-FR meldet „zahlreiche“ kompromittierte Fernsteuerungen von Kälteanlagen (Danfoss AK-SC/AK-SM, Copeland xweb, Dixell xweb) und hält die Kampagnen wahrscheinlich für noch nicht beendet.	100 %	100 %	bestätigt
Laut Public Sénat haben über 700 französische Supermärkte die Kontrolle über ihre Kühlanlagen verloren (Aussage in der Vorlage abgeschnitten, sinngemäß ergänzt).	100 %	95 %	präzisiert

Neu seit dem letzten Stand

• CERT-FR-Alert wurde am 16.10. nochmals aktualisiert (Empfehlungen), CISA und FBI warnen seit 5.11. ebenfalls

• BSI bezeichnet die Angriffe als „ungezielt und opportunistisch“ und bestätigt einen Pharmahändler in DE

• Schweizer Fall: Metzgerei in Köniz (BE) mit 50 bis 70 °C im Tiefkühler

• Bois-Guillaume als EFS-Standort konnte ich nicht bestätigen

• Seit 5.11. keine neuen offiziellen Angaben von EFS, Coolworld, Ministerium oder ANSSI gefunden

Wissensstand



Wissen 45 % Wahrscheinlich 24 % Nicht bekannt 31 %

Auswirkungen und Ablauf sind durch EFS, Ministerium und AFP gut belegt. Angriffsweg, Produkt, Täter und Zahl betroffener Geräte bleiben offen, und seit dem 5.11. habe ich keine neuen offiziellen Angaben gefunden (Stand 08.11.2026).

1. Was ist passiert, und warum?

WISSEN

• Das EFS bestätigt einen Cybervorfall bei einem „prestataire d'équipements frigorifiques“ am Montag, 2.11.2026. Manipuliert wurden Überwachungs- und Steuerungsanlagen von Kühlräumen an drei EFS-Standorten, Temperatur- und Abtauschwellen wurden auf sehr hohe Werte gesetzt. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

• Le Canard enchaîné nennt einen Sollwert von 110 °C statt rund minus 30 °C und den Dienstleister Coolworld. Die 110 °C sind ein eingestellter Sollwert, keine gemessene Temperatur im Kühlraum. (100 %) [https://www.it-connect.fr/cyberattaque-efs-coolworld-congelateurs-plasma/]

• Coolworld spricht in einer Mitteilung vom 4.11. von einer Schwachstelle in „un composant fourni par un prestataire tiers et non contrôlé directement par Coolworld“ und von wenigen betroffenen Geräten. Das EFS wird darin nicht namentlich genannt. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

• Laut Berichten betraf der Vorfall eine Software zur Fernüberwachung der Kühlsysteme (Remote Monitoring). (100 %) [https://esecurityplanet.com/threats/news-french-blood-bank-refrigeration-cyberattack-emea]

• SRF berichtet, die Täter seien über Coolworld in die Fernwartung eingedrungen. (100 %) [https://www.srf.ch/news/international/hintergruende-unklar-hackerangriff-auf-kuehlsysteme-blutbanken-in-frankreich-betroffen]

• Mindestens ein Standort liegt laut Canard und heise in Bourgogne-Franche-Comté. Die übrigen Standorte sind nicht offiziell genannt. (100 %) [https://www.heise.de/en/news/After-freezer-attacks-hackers-target-blood-bank-cooling-systems-11511459.html]

• NoName057(16) und Z-Pentest haben am 4.11. Angriffe auf Kühlsysteme europäischer Supermärkte per Telegram reklamiert. Für das EFS liegt mir keine belegte Bekennung vor. (100

%) [https://www.parismatch.be/actualites/societe/2026/11/04/cyberattaques-contre-des-supermarches-des-hackers-prorusses-revendiquent-les-attaques-QSYUP7ZMKBFHDNM72SWSVNOFBM/]

• Das BSI sieht keine Belege für die prorussische Zuschreibung und hält Trittbrettfahrer für möglich. Es bewertet die Angriffe als „ungezielt und opportunistisch“. (100 %) [https://correctiv.org/aktuelles/infrastruktur/2026/11/05/hackerangriffe-auf-kuehlsysteme-auch-pharmahaendler-in-deutschland-betroffen/]

NICHT BEKANNT

• Welches Produkt bzw. welche Drittanbieter-Komponente betroffen war

• Wie genau der Zugang erfolgte (Schwachstelle, Zugangsdaten, offen erreichbare Oberfläche)

• Wer die Täter sind und was sie wollten

• Ob das EFS gezielt oder zufällig als Kunde des Dienstleisters getroffen wurde

• Welche drei Standorte betroffen sind (Bois-Guillaume konnte ich in keiner Quelle finden)

WAHRSCHEINLICH (Einschätzung)

• Der Zugang lief über eine aus dem Internet erreichbare Fernwartungs- oder Überwachungsoberfläche des Dienstleisters. (70 %) – AFP/eSecurityPlanet nennen Fernüberwachungs-Software, SRF spricht von Fernwartung, Coolworld von einer Drittanbieter-Komponente. Ob die Oberfläche direkt offen war oder über ein Portal des Dienstleisters lief, ist nicht belegt.

• Gleiches Muster wie die Supermarkt-Welle (Sollwerte und Abtauung verstellt), vermutlich opportunistisch gefundene Systeme. (55 %) – Methode und Zeitpunkt (2.11., gleicher Tag wie neue Fälle in mehreren EU-Ländern) passen. Das BSI spricht von ungezielten Angriffen. Ein formaler Zusammenhang ist von keiner Behörde festgestellt.

• Gezielte staatliche Sabotage am Gesundheitswesen (12 %) – Keine Behörde spricht von gezielter Aktion, das BSI nennt die Welle opportunistisch, die Hacktivisten-Bekennung ist unbelegt und schließt das EFS nicht ausdrücklich ein.

2. Was ist die Auswirkung?

WISSEN

• Laut EFS „aucun impact sanitaire n'a été identifié“, kein Verlust von Blutprodukten. Überwachungs- und Alarmsysteme hätten die Anomalien rasch erkannt. (100 %) [https://www.francetinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

• In den Kühlräumen lagerten Plasmabeutel für Transfusionen und für die Arzneimittelherstellung durch Fraktionierung. Sie wurden vorsorglich in andere Anlagen verlegt. (100 %) [https://www.francetinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

• Ein Bereitschaftstechniker bemerkte den nächtlichen Temperaturanstieg rechtzeitig. (100 %) [https://www.srf.ch/news/international/hintergruende-unklar-hackerangriff-auf-kuehlsysteme-blutbanken-in-frankreich-betroffen]

• Laut Gesundheitsministerium gab es keine schwerwiegenden betrieblichen Folgen. (100 %) [https://www.techniques-ingenieur.fr/actualite/breves-afp/des-chambres-froides-de-letablissement-francais-du-sang-victimes-dune-cyberattaque-dun-prestataire-165616/]

• Plasma für Transfusionen muss bei minus 25 °C oder kälter gelagert werden. (100 %) [https://www.it-connect.fr/cyberattaque-efs-coolworld-congelateurs-plasma/]

NICHT BEKANNT

• Wie warm die Kühlräume tatsächlich wurden und wie lange

• Ob Plasma vorsorglich gesperrt oder nachgeprüft wurde

• Ob der Dienstleister weitere Kunden (Kliniken, Labore, Pharma) mit denselben Geräten betreut

WAHRSCHEINLICH (Einschätzung)

• Die Versorgung von Patienten mit Blutprodukten war nicht beeinträchtigt. (88 %) – EFS und Ministerium melden keinen Produktverlust und keine gesundheitlichen Folgen, die Ware wurde verlegt. Eine ausdrückliche Aussage zur Versorgungslage habe ich nicht gefunden.

• Ohne Alarmierung und Bereitschaft wäre Plasma verloren gegangen. (60 %) – Ein Sollwert deutlich über null hätte die Lagergrenze von minus 25 °C nach einigen Stunden überschritten. Wie schnell die Räume sich erwärmen, hängt von Raumgröße und Beladung ab, Messwerte gibt es nicht.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

• Laut Ministerium (Büro von Ministerin Stéphanie Rist) laufen die technischen Untersuchungen weiter, ein neuer Lagebericht soll folgen. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

• Die betroffenen Geräte wurden laut EFS „maîtrisés“ oder „neutralisés“. Das EFS arbeitet mit der ANSSI und dem Gesundheitsministerium zusammen und verstärkt die Überwachung. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

• Der Fernzugriff auf die betroffenen Kühlgeräte wurde laut Berichten abgeschaltet. (100 %) [https://esecurityplanet.com/threats/news-french-blood-bank-refrigeration-cyberattack-emea]

• CERT-FR schreibt zur Supermarkt-Welle: „N'effectuer qu'un Reset Factory est dans ce cas insuffisant“. Der Reset entfernt Persistenz, das Gerät bleibt aber verwundbar, solange es ohne Patch im Internet hängt. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

NICHT BEKANNT

• Ob es überhaupt einen IT-Ausfall beim EFS gab (berichtet wird nur der Dienstleister)

• Wann der Fernzugang wieder in Betrieb geht und in welcher Form

• Ob ein Patch für die Drittanbieter-Komponente existiert

WAHRSCHEINLICH (Einschätzung)

• Die Kühlung selbst läuft lokal weiter, offline ist vor allem der Fernzugang. (72 %) – Kälteregler arbeiten lokal, die Ware wurde verlegt, Geräte „neutralisés“. Dass einzelne Räume komplett außer Betrieb sind, ist möglich, wird aber nicht berichtet.

• Bis der Fernzugang sauber wieder aufgebaut ist (VPN, neue Zugangsdaten, Patch oder neue Hardware), dauert es Wochen. (45 %) – Bei den Supermärkten verlangt CERT-FR VPN und Updates. Ohne Kenntnis der Komponente und des Patch-Stands ist die Dauer nicht seriös abzuschätzen.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

• Laut EFS gab es keinen Verlust von Blutprodukten. (100 %) [https://www.heise.de/en/news/After-freezer-attacks-hackers-target-blood-bank-cooling-systems-11511459.html]

• Verändert wurden Sollwerte bzw. Temperatur- und Abtauschwellen in der Steuerung. Mechanische Schäden werden nirgends gemeldet. (100 %) [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

NICHT BEKANNT

• Ob Kompressoren, Verdampfer oder Heizstäbe durch Dauerabtauung belastet wurden

• Ob Geräte ausgetauscht werden

WAHRSCHEINLICH (Einschätzung)

• Mechanisch ist nichts dauerhaft kaputt, verändert wurde vor allem die Konfiguration. (68 %) – Früh erkannt, keine Schadensmeldung. Länger laufende Abtauheizung kann Komponenten belasten, das ist aber nicht berichtet.

• Einzelne Steuergeräte oder Komponenten werden ausgetauscht statt nur gepatcht. (35 %) – CERT-FR nennt End-of-Life-Geräte als besonders gefährdet. Ob die EFS-Geräte dazugehören, ist unbekannt.

5. Wie viele solcher Ziele gibt es?

WISSEN

• CERT-FR kennt „zahlreiche“ Kompromittierungen von Danfoss AK-SC/AK-SM, Copeland xweb und Dixell xweb und hält die Kampagnen vermutlich für noch nicht beendet (Alert vom 12.10., aktualisiert 13. und 16.10.2026). (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Laut Public Sénat bzw. Regierung verloren rund 700 von etwa 10.000 französischen Supermärkten die Kontrolle über ihre Kältesteuerung. ANSSI-Chef Vincent Strubel nannte vor dem Senat elementare Sicherheitsmängel und schwache Passwörter als Ursache. (100 %) [https://www.publicsenat.fr/actualites/politique/des-defauts-de-securisation-elementaire-et-des-mots-de-passe-faibles-ont-permis-la-cyberattaque-contre-les-frigos-de-supermarches]

• In Deutschland sind dem BSI einzelne Vorfälle bei Supermärkten und in der Pharmabranche bekannt, darunter ein Pharmahändler mit Medikamentenkühlung. (100 %) [https://correctiv.org/aktuelles/infrastruktur/2026/11/05/hackerangriffe-auf-kuehlsysteme-auch-pharmahaendler-in-deutschland-betroffen/]

• In der Schweiz hat eine Metzgerei in Köniz (BE) nach manipulierten Kühl- und Tiefkühlgeräten 50 bis 70 °C gemeldet und eine Filiale vorübergehend geschlossen. (100 %) [https://www.20min.ch/story/koeniz-be-filiale-musste-schliessen-hacker-greifen-berner-metzgerei-an-103662735]

• CISA, FBI und weitere US-Behörden haben am 5.11. vor Angriffen auf industrielle Kühl- und Kühlkettenüberwachung gewarnt. (100 %) [https://www.malwarebytes.com/de/blog/news/2026/11/attacks-on-supermarket-and-blood-storage-systems-prompt-us-warning]

• Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 141314 gesamt (DNP3 31930, OMRON FINS 26209, ProConOS 15790, EtherNet/IP 15508, Siemens S7 7674, OPC UA 5015) (100 %)

NICHT BEKANNT

• Wie viele Kühlräume im Gesundheitswesen (Blutbanken, Kliniken, Apotheken, Labore) in DACH über Fernwartung erreichbar sind

• Eine offizielle Zahl offen erreichbarer Kältesteuerungen in DE/AT/CH

• Ob die Coolworld-Komponente zu den vom CERT-FR genannten Produkten gehört

WAHRSCHEINLICH (Einschätzung)

• In DACH sind mehrere Tausend gewerbliche Kälte- und Kühlkettensysteme über Fernwartung erreichbar, ein Teil davon direkt aus dem Internet. (65 %) – Fernüberwachung ist in der Kältetechnik Standard, Medien nennen zweistellige Tausenderzahlen offener Oberflächen weltweit (nicht von mir an der Primärquelle geprüft). Eine belastbare DACH-Zahl fehlt.

• Auch Kühlräume in deutschen Krankenhäusern oder Blutspendediensten werden über Dienstleister-Fernzugänge betreut. (75 %) – Übliches Wartungsmodell in der Branche. Konkrete Fälle sind öffentlich nicht belegt.

6. Kann das wieder passieren?

WISSEN

• CERT-FR hält die Kampagnen vermutlich für noch nicht beendet und warnt, dass Geräte ohne Patch nach einem Reset erneut kompromittiert werden. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Am 2.11. wurden neue Fälle aus mehreren europäischen Ländern gemeldet (u. a. Belgien, Luxemburg, Schweden, Irland, Niederlande, Estland). (100 %) [https://mesinfos.fr/don-du-sang-des-hackers-tentent-de-faire-chauffer-les-chambres-froides-de-l-efs-342575.html]

• Das BSI rät, Kältesteuerungen nicht direkt aus dem Internet erreichbar zu betreiben bzw. abzusichern und zu patchen. (100 %) [https://www.heise.de/en/news/After-freezer-attacks-hackers-target-blood-bank-cooling-systems-11511459.html]

NICHT BEKANNT

• Ob die Lücke bei Coolworld geschlossen ist

• Ob die Täter weitere Zugänge haben

WAHRSCHEINLICH (Einschätzung)

• Es gibt in den kommenden Wochen weitere Fälle in Europa, auch in DACH. (80 %) – Welle läuft seit Oktober in Schüben, CERT-FR erwartet Fortsetzung, CH und DE haben bereits Einzelfälle.

• Ein weiterer Fall trifft das Gesundheitswesen (Klinik, Labor, Pharma) in DACH. (45 %) – Pharmahändler in DE ist schon betroffen. Kliniken nutzen ähnliche Fernwartung, aber Treffer hängen davon ab, welche Systeme offen sind.

Lage

In der Nacht vom 1. auf den 2.11.2026 haben Angreifer über einen Kältetechnik-Dienstleister die Überwachung und Steuerung von Kühlräumen an drei Standorten des französischen Blutspendedienstes EFS manipuliert und Temperatur- und Abtauschwellen auf sehr hohe Werte gesetzt (laut Le Canard enchaîné ein Sollwert von 110 °C statt minus 30 °C). Laut EFS haben Alarme und Bereitschaftspersonal rechtzeitig reagiert, kein Blutprodukt ging verloren, die Plasmabeutel wurden verlegt. Der Fall gehört in eine europaweite Welle gegen internetfähige Kältesteuerungen, die Täter sind unbekannt, die Bekennung prorussischer Gruppen ist nicht belegt, und eine technische Ursache außer „Schwachstelle in einer Drittanbieter-Komponente“ (Coolworld) ist nicht veröffentlicht.

Angriff	Manipulation von Sollwerten sowie Temperatur- und Abtauschwellen in der Fernüberwachung/Steuerung von Kühlräumen an drei EFS-Standorten über einen Kältetechnik-Dienstleister (laut Canard enchaîné Coolworld). Keine Datenverschlüsselung, kein Datenabfluss berichtet.
Wann / Status	Nacht 1. auf 2.11.2026 (EFS nennt Montag, 2.11.), öffentlich am 3.11. durch Le Canard enchaîné, EFS-Bestätigung 3.11. abends, Coolworld-Mitteilung 4.11. · eingedämmt
Täter	Unbekannt. NoName057(16) und Z-Pentest reklamieren die Supermarkt-Welle, für das EFS liegt keine belegte Bekennung vor. BSI sieht keine Belege und hält Trittbrettfahrer für möglich. – unbekannt
Betreiber / Branche	Établissement français du sang (EFS) über Dienstleister Coolworld (Name laut Canard enchaîné) · Gesundheitswesen, Blutspende und Blutprodukte
Anlage / Alter	Kühl- bzw. Tiefkühlräume für Plasma (ca. minus 30 °C) mit Fernüberwachung des Dienstleisters ·
Region	Frankreich, drei Standorte, mindestens einer laut Canard in Bourgogne-Franche-Comté
Auswirkungen	Laut EFS und Ministerium keine gesundheitlichen Folgen, kein Verlust von Blutprodukten, Plasma vorsorglich umgelagert. Eine Beeinträchtigung der Patientenversorgung ist nicht berichtet. Das Risiko lag im Verlust von Transfusions- und Fraktionierungsplasma, das sich nicht kurzfristig ersetzen lässt.
Behörden	ANSSI und französisches Gesundheitsministerium (Ministerin Stéphanie Rist) arbeiten mit dem EFS, CERT-FR hat zur Welle gewarnt. In DE äußert sich das BSI, in den USA CISA und FBI. Kantonspolizei Bern ermittelt zum Fall Köniz.
Regulatorik	Frankreich: Einstufung des EFS als OIV/OSE und Stand der NIS2-Umsetzung habe ich nicht geprüft. Für DE: Blut- und Plasmaversorgung gehört zum KRITIS-Sektor Gesundheit, Betreiber oberhalb der Schwellen müssen erhebliche Störungen an das BSI melden (nicht in dieser Recherche geprüft). Nach NIS2 gelten Frühwarnung binnen 24 Stunden und Meldung binnen 72 Stunden, Art. 21 verlangt Sicherheit in der Lieferkette, also auch für Wartungsdienstleister mit Fernzugang. Der CRA verpflichtet künftig Hersteller vernetzter Steuerungen zu Updates und Schwachstellenmanagement.

Angriffsvektor

Bekannt: Laut Coolworld eine Schwachstelle in einer Drittanbieter-Komponente, laut AFP-Berichten betroffen war eine Fernüberwachungs-Software. Produkt und Ausnutzungsweg sind nicht veröffentlicht.

• Schwachstelle in einer internetseitig erreichbaren Fernüberwachungs- oder Cloud-Komponente des Drittanbieters (hoch): Deckt sich mit der Coolworld-Aussage. Für Kälte-Managementsysteme sind mehrere Schwachstellen öffentlich (u. a. Copeland XWEB Pro, Danfoss AK-SM), CERT-FR warnt vor ungepatchten End-of-Life-Geräten.

• Schwache oder Standard-Zugangsdaten an Kältesteuerungen bzw. am Fernwartungsportal (mittel): ANSSI nannte bei der Supermarkt-Welle schwache Passwörter und elementare Mängel. Coolworld spricht dagegen von einer Schwachstelle, nicht von Passwörtern.

• Kompromittierter Zugang beim Dienstleister selbst (gestohlene Zugangsdaten, Lateral Movement vom Dienstleisternetz zu Kundenanlagen) (gering): Würde mehrere Standorte gleichzeitig erklären, wird aber von keiner Quelle berichtet und passt weniger zur Aussage „wenige Geräte“.

Zeitleiste

12.10.2026 CERT-FR veröffentlicht Alert CERTFR-2026-ALE-012 zu kompromittierten Kältesteuerungen (Danfoss AK-SC/AK-SM), Updates am 13.10. (Copeland/Dixell xweb ergänzt) und 16.10. – bestätigt [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

13.10.2026 Danfoss rät niederländischen Kunden, Systeme vom öffentlichen Internet zu trennen – berichtet [https://www.malwarebytes.com/de/blog/news/2026/11/attacks-on-supermarket-and-blood-storage-systems-prompt-us-warning]

21.10.2026 ANSSI-Chef Strubel vor dem Senat: elementare Mängel und schwache Passwörter, rund 700 Supermärkte betroffen – berichtet [https://www.publicsenat.fr/actualites/politique/des-defauts-de-securisation-elementaire-et-des-mots-de-passe-faibles-ont-permis-la-cyberattaque-contre-les-frigos-de-supermarches]

Nacht 1. auf 2.11.2026 Sollwerte und Abtauschwellen an drei EFS-Standorten verstellt, Bereitschaftstechniker bemerkt Temperaturanstieg – bestätigt [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

2.11.2026 Neue Fälle an Supermarkt-Kühlungen in mehreren EU-Ländern gemeldet – berichtet [https://mesinfos.fr/don-du-sang-des-hackers-tentent-de-faire-chauffer-les-chambres-froides-de-l-efs-342575.html]

3.11.2026 Le Canard enchaîné macht den Fall öffentlich (110 °C, Coolworld), EFS bestätigt per Mitteilung – bestätigt [https://www.franceinfo.fr/internet/securite-sur-internet/cyberattaques/une-cyberattaque-touche-des-installations-frigorifiques-utilisees-par-l-etablissement-francais-du-sang-sans-impact-sur-les-echantillons-conserves_8267426.html]

4.11.2026 Coolworld nennt Schwachstelle in Drittanbieter-Komponente, Ministerium: Untersuchungen laufen. NoName057(16)/Z-Pentest reklamieren die Supermarkt-Angriffe. – berichtet [https://www.parismatch.be/actualites/societe/2026/11/04/cyberattaques-contre-des-supermarches-des-hackers-prorusses-revendiquent-les-attaques-QSYUP7ZMKBFHDNM72SWSVNOFBM/]

5.11.2026 BSI bestätigt Einzelfälle in DE inkl. Pharmahändler, CISA/FBI warnen, Metzgerei in Köniz (CH) betroffen – berichtet [https://correctiv.org/aktuelles/infrastruktur/2026/11/05/hackerangriffe-auf-kuehlsysteme-auch-pharmahaendler-in-deutschland-betroffen/]

6. bis 8.11.2026 Keine neuen offiziellen Angaben von EFS, Coolworld oder ANSSI gefunden – vermutet [https://esecurityplanet.com/threats/news-french-blood-bank-refrigeration-cyberattack-emea]

Vergleichsfälle

• Kältesteuerungen in rund 700 französischen Supermärkten manipuliert (2026): Offen erreichbare Steuerungen mit Standardpasswörtern reichen für flächige Sabotage ohne jede Malware. [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Pharmahändler in Deutschland, Medikamentenkühlung angegriffen (2026): Die Welle hat die Kühlkette für Arzneimittel in DE bereits erreicht. [https://correctiv.org/aktuelles/infrastruktur/2026/11/05/hackerangriffe-auf-kuehlsysteme-auch-pharmahaendler-in-deutschland-betroffen/]

• Metzgerei in Köniz (BE), Tiefkühler auf 50 bis 70 °C (2026): Auch kleine Betriebe in der Schweiz sind betroffen, nicht nur große Ketten. [https://www.20min.ch/story/koeniz-be-filiale-musste-schliessen-hacker-greifen-berner-metzgerei-an-103662735]

• Wasserwerk Oldsmar (Florida), Sollwert Natronlauge per Fernzugriff verstellt (2021): Ein aufmerksamer Mitarbeiter und Plausibilitätsgrenzen verhinderten Schaden, genau wie jetzt beim EFS. [https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a]

• Unitronics-Steuerungen in US-Wasserwerken (u. a. Aliquippa) über Standardpasswort übernommen (2023): Hacktivisten suchen gezielt offen erreichbare Steuerungen und nutzen Standardzugänge. [https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a]

Begriffe einfach erklärt

OT: Operational Technology, also die Technik, die physische Anlagen wie Kühlräume, Pumpen oder Maschinen steuert.

Sollwert: Die Temperatur, auf die eine Anlage regeln soll, hier normalerweise rund minus 30 Grad.

Abtauung: Ein Heizbetrieb, mit dem Kühlgeräte regelmäßig das Eis vom Verdampfer entfernen; wer ihn missbraucht, heizt den Kühlraum auf.

Fernwartung: Zugang, über den ein Dienstleister die Anlage aus der Ferne überwacht und einstellt.

CERT-FR / ANSSI: Die französische Cybersicherheitsbehörde und ihr Warn- und Reaktionsteam, vergleichbar mit dem BSI.

Fraktionierung: Verfahren, mit dem aus Blutplasma Medikamente wie Gerinnungsfaktoren hergestellt werden.

Früherer Stand: Erstmeldung (05.11.2026 10:35)

Wissen 43 % · wahrscheinlich 25 % · nicht bekannt 32 %

In der Nacht vom 1. auf den 2. November 2026 haben Angreifer über die Fernüberwachung und Fernsteuerung eines Kältetechnik-Dienstleisters die Temperatur- und Abtauschwellen von Kühlräumen an drei Standorten des französischen Blutspendedienstes EFS auf sehr hohe Werte gesetzt. Le Canard enchaîné nennt den Dienstleister Coolworld und einen Sollwert von 110 °C statt minus 30 °C. Das EFS hat nur „sehr hohe Temperaturen“ bestätigt, keine Zahl. Unabhängige Alarmsysteme und ein Bereitschaftstechniker haben den Vorfall laut EFS rasch erkannt, Produkte gingen nicht verloren. Der Fall gehört zeitlich zu einer Angriffswelle auf Kältesteuerungen in Supermärkten in Frankreich (Oktober) und Deutschland (Anfang November), ein technischer Zusammenhang ist aber nicht belegt.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.