VORFALL-LAGEBILD

Pentagon untersucht Gefriertruhen-Ausfälle auf US-Militärbasen als mutmaßlichen Cyberangriff

Stand 12.11.2026 15:49 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Nach bisherigem Stand sind die US-Fälle nicht offiziell als Hack bestätigt, das Muster gleicht aber den bestätigten Angriffen in Europa.

2. Seit dem 2. November sind auch Supermärkte in Deutschland betroffen, und die Ursache sitzt meist in einer Steuerung, die offen im Internet hängt oder per Fernwartung erreichbar ist.

3. Kleine Betreiber kommen mit wenigen Schritten weit: Steuerung raus aus dem Internet, Fernwartung absichern, Temperaturalarme einrichten und wissen, was im Notfall zu tun ist.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Das Verteidigungsministerium bestätigte am 28.08.2026 eine „possible refrigeration disruption at some Defense Commissary Agency commissaries“. Die Ware wurde in andere gekühlte Bereiche gebracht, die Märkte blieben offen.	100 %	100 %	bestätigt
Fort Huachuca (Arizona) meldete, die Gefriertruhen seien trotz durchgehender Stromversorgung in den Abtaumodus gegangen. Reuters nennt den 26.08. als Datum der Meldung, der Blog Signal and Silence den 27.08.	100 %	100 %	bestätigt
Laut vier Beamten behandelt das Pentagon die Ausfälle als mutmaßlichen Hack (berichtet, anonym).	100 %	100 %	bestätigt
Army CID (Cyber Field Office) und Air Force OSI bestätigten Ermittlungen, die Federführung hat laut Air Force der DCIS.	100 %	95 %	präzisiert
Die Ausfälle gehen auf eine Fernmanipulation an der Kältesteuerung zurück und nicht auf zufällige Defekte.	65 %	70 %	offen
Die Vorfälle in den USA und in Frankreich hängen technisch oder über denselben Threat Actor zusammen.	40 %	45 %	offen
Lebensmittel verdarben, in mindestens einem Fall wurden die Kühlaggregate über Nacht hochgeregelt.	100 %	100 %	bestätigt
Reuters zählt mindestens sechs betroffene Commissaries, darunter Fort Huachuca und Fort Irwin. Military Times nennt u. a. Holloman, Newport, Little Rock, F.E. Warren und Robins; ein Social-Media-Account sprach von 18, das ist unbestätigt.	100 %	100 %	präzisiert

Frühere Aussage	vorher	jetzt	Status
Laut Stars and Stripes ging es um Ware im Wert von Tausenden Dollar.	100 %	95 %	bestätigt
Die Märkte blieben geöffnet.	100 %	100 %	bestätigt
Der direkte Schaden in den USA bleibt im Bereich verdorbener Ware und kurzer Engpässe, ohne Folgen für die militärische Einsatzfähigkeit.	75 %	75 %	offen
Laut Mitarbeiterangaben waren einzelne Standorte wie NAS Lemoore (28.08.), Naval Station Newport und Dyess (29.08.) nach ein bis drei Tagen wieder in Betrieb (Angaben aus Blog, teils unbestätigt).	100 %	95 %	bestätigt
CERT-FR empfiehlt für kompromittierte Geräte: vom Internet trennen, neu starten oder auf Werkseinstellungen setzen, neu konfigurieren, Firmware aktualisieren. Ein Reset allein reicht nicht, ein ungepatchtes Gerät mit Internetzugang wird sehr wahrscheinlich erneut kompromittiert.	100 %	100 %	bestätigt
Die reine Wiederherstellung des Kühlbetriebs dauert Stunden bis wenige Tage, die saubere Bereinigung und Absicherung aller Standorte Wochen.	70 %	70 %	offen
In Frankreich wurden einige Geräte so stark erhitzt, dass sie Feuer fingen; gemeldete Brände untersucht die Pariser Staatsanwaltschaft.	100 %	100 %	bestätigt
In Frankreich blieben einige Kühl- und Tiefkühlvitrinen außer Betrieb.	100 %	100 %	bestätigt
Der Kühlgeräte-Lieferant Aldevra bekam laut Stars and Stripes keine Serviceanfragen zu den US-Ausfällen.	100 %	100 %	bestätigt
In den US-Commissaries ist keine dauerhafte Hardware-Schädigung entstanden.	70 %	65 %	offen
Ältere Steuerungen ohne Sicherheitsupdates müssen ersetzt werden, was wegen Lieferzeiten und Kältetechniker-Kapazität Wochen bis Monate dauern kann.	60 %	70 %	präzisiert
Die Defense Commissary Agency betreibt rund 235 Märkte in 13 Ländern.	100 %	100 %	bestätigt
Forescout fand weltweit 6.017 öffentliche IP-Adressen mit exponierten Kältesteuerungen in 99 Ländern (u. a. Copeland/Dixell XWEB 7.075 Dienste, Danfoss StoreView 4.697).	100 %	100 %	bestätigt
Claroty berichtete laut Fachpresse von 2.765 per Censys gefundenen, aus dem Internet erreichbaren Geräten; das sagt nichts über die Firmware-Version.	100 %	100 %	bestätigt
In Frankreich waren laut Finanzminister Roland Lescure rund 700 der etwa 10.000 Supermärkte betroffen; Reuters nennt mehr als 350 Einrichtungen.	100 %	100 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
Im DACH-Raum sind mehrere hundert Kältesteuerungen … (Aussage in der Vorlage abgeschnitten)	unbekannt %	60 %	offen

Neu seit dem letzten Stand

• Zweite Angriffswelle am 02.11.2026 in rund einem Dutzend Ländern, darunter Deutschland (Reisbach, Raesfeld, Wuppertal, Wetter-Volmarstein, Lilienthal).

• Nextgov (29.10.): Zwei anonyme Quellen nennen einen Iran-Verdacht für die US-Vorfälle.

• Gemeinsames Factsheet von CISA, FBI, HHS, USDA und DOT am 05.11.2026 mit Warnung vor laufender Bedrohung.

• Army CID arbeitet mit französischen Strafverfolgern zusammen.

• In Frankreich traf ein Angriff auch die Kühlung von Blutkonserven und wurde rechtzeitig gestoppt.

• Belgiens Föderalstaatsanwaltschaft und die Kripo Landshut ermitteln.

Wissensstand



■ Wissen 48 % ■ Wahrscheinlich 24 % ■ Nicht bekannt 28 %

Die Angriffe in Europa sind von Behörden bestätigt (CERT-FR, Belgiens Föderalstaatsanwaltschaft, deutsche Kripo-Ermittlungen). Für die US-Militärbasen gibt es dagegen nur anonyme Quellen, eine offizielle Bestätigung als Cyberangriff fehlt, und Täter und Einfallsweg sind offen.

1. Was ist passiert, und warum?

WISSEN

• Das Verteidigungsministerium bestätigte am 28.08.2026 eine „possible refrigeration disruption at some Defense Commissary Agency commissaries“. (100 %)
[https://militarytimes.com/news/your-military/2026/08/28/dod-confirms-refrigeration-disruption-at-military-commissaries/]

• Fort Huachuca schrieb, der Gefrierschrank sei „in defrost mode“ gegangen, „where it heated up all the food“. In einem Fall wurden Kühlaggregate über Nacht auf Heizen gestellt. (100 %) [https://www.militarytimes.com/pentagon/2026/10/29/pentagon-treating-military-base-freezer-malfunctions-as-suspected-cyberattack-officials-say/]

• Laut vier Beamten (Reuters, anonym) behandelt das Pentagon die Ausfälle als mutmaßlichen Hack. Offiziell lehnt das Pentagon unter Verweis auf die laufenden Ermittlungen jede Auskunft ab. (100 %) [https://taskandpurpose.com/news/military-commissary-cyberattack-pentagon-investigation/]

• Die Ermittlungen führt der DCIS. Die Army CID (Cyber Field Office) ist beteiligt und arbeitet mit französischen Strafverfolgern zusammen. Eine Einheit von US Cyber Command erklärt, sie arbeite „in close coordination with interagency and law enforcement partners“. (100 %) [https://www.militarytimes.com/pentagon/2026/10/29/pentagon-treating-military-base-freezer-malfunctions-as-suspected-cyberattack-officials-say/]

• Laut zwei anonymen Quellen vermuten US-Beamte Iran-nahe Hacker hinter den Angriffen. Eine offizielle Zuordnung gibt es nicht. (100 %)
[https://www.nextgov.com/cybersecurity/2026/10/officials-suspect-iran-series-cyberattacks-military-base-freezers/416934/]

NICHT BEKANNT

• Ob es tatsächlich ein Cyberangriff war: offiziell nicht bestätigt, und die Ermittler haben laut Berichten noch nicht geklärt, ob Steuerungen kompromittiert wurden.

• Einfallsweg (Initial Access) und Täter.

• Welcher Hersteller in den Commissaries verbaut ist; Reuters konnte Danfoss oder eine andere Marke nicht bestätigen.

• Wie weit die Ermittlungen sind.

WAHRSCHEINLICH (Einschätzung)

• Die Ausfälle gehen auf eine Fernmanipulation der Kältesteuerung zurück und nicht auf zufällige Defekte. (70 %) – Mehrere Standorte fielen zeitnah mit demselben Muster aus (Abtauen oder Heizen über Nacht trotz Strom). Das Muster entspricht genau dem, was CISA und CERT-FR für die bestätigten Angriffe beschreiben. Eine offizielle Bestätigung fehlt.

• Die US-Vorfälle und die Wellen in Europa gehen auf denselben Threat Actor zurück. (45 %) – Das Vorgehen ist gleich, und für beide Fälle wird inoffiziell Iran vermutet. Bisher wurde aber kein technischer Zusammenhang belegt, und die US-Vorfälle liegen sechs Wochen vor der französischen Welle.

• Ein staatlich unterstützter iranischer Akteur steckt hinter den US-Vorfällen. (40 %) – Es gibt nur zwei anonyme Quellen, laut NPR-basierten Berichten ohne hohe Konfidenz. Iran ist in der Vergangenheit bereits mit Angriffen auf internetexponierte OT aufgefallen.

2. Was ist die Auswirkung?

WISSEN

• Mindestens sechs Commissaries waren betroffen, Fleisch, Molkereiprodukte, Obst, Gemüse und Tiefkühlware verdarben. Nicht bestätigte Quellen sprechen von bis zu zwölf Märkten. (100 %) [https://www.stripes.com/theaters/us/2026-11-04/cyber-attacks-commissary-freezers-23362522.html]

• Das Pentagon nennt weder die Zahl der betroffenen Märkte noch den Schaden. (100 %) [https://www.stripes.com/theaters/us/2026-11-04/cyber-attacks-commissary-freezers-23362522.html]

• In Deutschland entsorgte ein Händler in Lilienthal nach eigenen Angaben Ware für über 360.000 Euro; in Reisbach mussten laut Marktleitung „Unmengen an Lebensmitteln in die Tonne“. (100 %) [https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

• In Frankreich wurde auch die Temperatur in Kühleinheiten mit Blutkonserven erhöht. Der Angriff wurde gestoppt, bevor die Blutbestände in Gefahr waren. (100 %) [https://techcrunch.com/2026/11/05/u-s-government-warns-of-ongoing-cyber-threat-amid-mass-hacks-of-industrial-retail-and-military-freezers]

• Laut CISA-Factsheet können veränderte Temperaturen die Lebensdauer der Anlagen verkürzen, Brandgefahr erzeugen und Verbraucher über unsicher gelagerte Produkte gefährden. Möglich ist auch ein Verlust der Temperatursicht (denial of view). (100 %) [https://www.cisa.gov/resources-tools/resources/us-government-partners-urge-hardening-industrial-refrigeration-and-cold-chain-monitoring-systems]

NICHT BEKANNT

• Gesamtschaden in den USA.

• Ob verdorbene Ware verkauft wurde (keine Berichte darüber gefunden).

WAHRSCHEINLICH (Einschätzung)

• Der direkte Schaden in den USA beschränkt sich auf verdorbene Ware und kurze Engpässe, die militärische Einsatzfähigkeit war nicht betroffen. (75 %) – Die Märkte blieben offen und die Ware wurde umgelagert. Es gibt keine Berichte über Folgen für Truppenverpflegung oder Einsatz.

• Die Wirkung liegt vor allem in der Botschaft: Versorgung auf Militärbasen ist über billige Gebäudetechnik angreifbar. (60 %) – Das ist eine Einschätzung aus dem geringen Sachschaden und der großen Medienresonanz. Ein Motiv ist nicht belegt.

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

WISSEN

• CERT-FR empfiehlt: Internetzugang der Geräte trennen, Zugriff nur über abgesichertes VPN, komplette Konfiguration inklusive Abtaupläne prüfen, Firmware aktualisieren, bei Danfoss den Sicherheitsmodus „Strict“ setzen, Standardpasswörter ändern. Kompromittierte Geräte neu starten oder auf Werkseinstellungen setzen und neu konfigurieren. Ein Reset allein reicht nicht. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Laut CERT-FR laufen die Angriffskampagnen wahrscheinlich weiter. End-of-Life-Geräte ohne Patches mit Internetzugang sind sehr stark gefährdet. (100 %) [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

• Laut Mitarbeiterangaben aus einem Blog waren einzelne US-Standorte nach ein bis drei Tagen wieder in Betrieb (teils unbestätigt). (100 %) [https://www.militarytimes.com/?p=158929]

NICHT BEKANNT

• Wie die US-Standorte bereinigt wurden.

• Ob Logs vorhanden sind, mit denen sich der Zugriff rekonstruieren lässt.

WAHRSCHEINLICH (Einschätzung)

• Den Kühlbetrieb wiederherzustellen dauert Stunden bis wenige Tage, die saubere Bereinigung und Absicherung aller Standorte dagegen Wochen. (70 %) – Die Steuerung lässt sich schnell zurückstellen. Die Inventur aller Fernwartungszugänge, Firmware-Updates und Gerätetausch brauchen aber Kältetechniker vor Ort.

• Ohne Logs auf den Geräten wird sich der genaue Einfallsweg an manchen Standorten nicht mehr klären lassen. (55 %) – CISA empfiehlt ausdrücklich, Logging einzuschalten oder ersatzweise den Netzverkehr mitzuschneiden. Das deutet darauf hin, dass Logs häufig fehlen.

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

WISSEN

• Laut Danfoss waren viele der in Frankreich betroffenen Geräte veraltet oder liefen mit alter Firmware. (100 %) [https://www.militarytimes.com/pentagon/2026/10/29/pentagon-treating-military-base-freezer-malfunctions-as-suspected-cyberattack-officials-say/]

• Für ältere Danfoss-Hardware gibt es keine Sicherheitsupdates mehr. (100 %) [https://techcrunch.com/2026/11/05/u-s-government-warns-of-ongoing-cyber-threat-amid-mass-hacks-of-industrial-retail-and-military-freezers]

• CISA empfiehlt, End-of-Life-Geräte zu identifizieren und zu ersetzen, und warnt vor verkürzter Lebensdauer der Anlage und Brandgefahr. (100 %) [https://www.cisa.gov/resources-tools/resources/us-government-partners-urge-hardening-industrial-refrigeration-and-cold-chain-monitoring-systems]

NICHT BEKANNT

• Ob in den US-Commissaries Hardware beschädigt wurde.

• Welche Steuerungsgenerationen dort laufen.

WAHRSCHEINLICH (Einschätzung)

• In den US-Commissaries ist keine dauerhafte Hardware-Schädigung entstanden. (65 %) – Der Kühlgeräte-Lieferant Aldevra bekam keine Serviceanfragen, und Standorte liefen nach Tagen wieder. CISA nennt aber verkürzte Lebensdauer als mögliche Folge.

• Veraltete Steuerungen ohne Updates müssen ersetzt werden, was wegen Lieferzeiten und knapper Kältetechniker Wochen bis Monate dauern kann. (70 %) – Danfoss liefert für alte Hardware keine Patches mehr, CERT-FR und CISA raten zum Tausch, und Hunderte Märkte brauchen gleichzeitig dieselben Techniker.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Die Defense Commissary Agency betrieb Ende September 2024 rund 235 Märkte in 13 Ländern und 2 US-Territorien. (100 %) [https://www.congress.gov/crs_external_products/IF/PDF/IF11089/IF11089.18.pdf]

• Forescout fand am 22.10.2026 weltweit 6.017 öffentliche IP-Adressen mit exponierten Kältesteuerungen in 99 Ländern (Dienste: Copeland/Dixell XWEB 7.075, Danfoss StoreView 4.697). (100 %)
[https://www.forescout.com/blog/cold-chain-open-control-exposed-refrigeration-systems-reveal-global-risk/]

• In Frankreich waren laut Reuters mehr als 350 Einrichtungen betroffen; Finanzminister Lescure sprach laut AP von rund 700 der etwa 10.000 Supermärkte. (100 %) [https://www.militarytimes.com/pentagon/2026/10/29/pentagon-treating-military-base-freezer-malfunctions-as-suspected-cyberattack-officials-say/]

• Die zweite Welle am 02.11. traf allein in Belgien mindestens 76 Geschäfte, darunter rund 40 Delhaize-Filialen. (100 %)
[https://www.helpnetsecurity.com/2026/11/02/european-supermarkets-refrigeration-units-cyberattacks/]

• Am 02.11. waren unter anderem Schweden, Belgien, Estland, Luxemburg, Italien, Irland, die Niederlande, Portugal und Deutschland betroffen. (100 %)

[https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

• Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 140110 gesamt (DNP3 31683, OMRON FINS 26391, ProConOS 15525, EtherNet/IP 15295, Siemens S7 7580, OPC UA 4964) (100 %)

NICHT BEKANNT

• Wie viele exponierte Kältesteuerungen es in Deutschland, Österreich und der Schweiz gibt; die Länderzahlen von Forescout stehen nur in einer Grafik und wurden hier nicht ausgewertet.

• Die Zahl der betroffenen Märkte in Deutschland insgesamt.

WAHRSCHEINLICH (Einschätzung)

• In Deutschland gibt es mehr betroffene Märkte als die fünf öffentlich bekannten. (65 %) – Bekannt sind Fälle nur dort, wo Inhaber selbst an die Öffentlichkeit gegangen sind. Filialisten melden Einzelfälle selten.

6. Kann das wieder passieren?

WISSEN

• CISA, FBI, HHS, USDA und DOT sprechen am 05.11.2026 von einer laufenden Bedrohung. Laut CISA sollte jede Organisation mit Kühl- und Überwachungssystemen davon ausgehen, ein Ziel zu sein. (100 %) [https://techcrunch.com/2026/11/05/u-s-government-warns-of-ongoing-cyber-threat-amid-mass-hacks-of-industrial-retail-and-military-freezers]

• Die zweite Welle folgte drei Wochen nach der ersten (12.10. Frankreich, 02.11. rund ein Dutzend Länder). (100 %)

[https://www.helpnetsecurity.com/2026/11/02/european-supermarkets-refrigeration-units-cyberattacks/]

• Das BSI hat Betreiber aufgerufen, aus dem Internet erreichbare Steuerungen nach Stand der Technik abzusichern. (100 %)

[https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

NICHT BEKANNT

• Ob und wann eine dritte Welle kommt.

• Ob der Täter auch andere Gebäude- und Betriebstechnik (Heizung, Lüftung) ins Visier nimmt.

WAHRSCHEINLICH (Einschätzung)

• Es wird weitere Angriffe auf exponierte Kältesteuerungen geben. (85 %) – Zwei Wellen in drei Wochen, Tausende Geräte weiterhin offen erreichbar, alte Geräte ohne Patch, und Behörden sprechen von einer laufenden Kampagne.

• Nachahmer nutzen die bekannte Methode ebenfalls. (55 %) – Das BSI warnte ausdrücklich vor Nachahmern. Belege für Trittbrettfahrer gibt es bisher nicht.

Lage

Ende August 2026 gingen in mindestens sechs Commissaries (Lebensmittelmärkte auf US-Militärbasen) die Tiefkühlgeräte über Nacht in den Abtaumodus, die Lebensmittel verdarben. Laut Reuters behandelt das Pentagon die Ausfälle als mutmaßlichen Hack, offiziell bestätigt ist das nicht. Zwei anonyme Quellen nennen gegenüber Nextgov einen Iran-Verdacht. Parallel wurden in Frankreich (11./12.10.) und in einer zweiten Welle am 02.11. in rund einem Dutzend europäischer Länder Kältesteuerungen manipuliert, darunter auch in Deutschland (Reisbach, Raesfeld, Wuppertal, Wetter-Volmarstein, Lilienthal). Am 05.11. warnten CISA, FBI, HHS, USDA und DOT gemeinsam vor laufenden Angriffen auf Kältesteuerungen.

Angriff	Manipulation von Kälte- und Tiefkühlsteuerungen (Abtau- oder Heizbetrieb über Nacht), Lebensmittel verdarben; in den USA nicht offiziell als Cyberangriff bestätigt
Wann / Status	USA Ende August 2026 (ab ca. 26.08.); Frankreich 11./12.10.2026; Europa inkl. Deutschland 02.11.2026 · laufend
Täter	Unbekannt; zwei anonyme Quellen nennen einen Iran-Verdacht für die US-Vorfälle, keine offizielle Zuordnung, kein Bekennerschreiben – vermutet

Betreiber / Branche	Defense Commissary Agency (DeCA), mindestens sechs Commissaries, u. a. Fort Huachuca (AZ) und Fort Irwin (CA) · Lebensmittelhandel für Militärangehörige (Bundesbehörde, US-Verteidigungsministerium)
Anlage / Alter	Kühl- und Tiefkühlanlagen mit vernetzter Kältesteuerung ·
Region	USA
Auswirkungen	Verdorbene Lebensmittel und kurze Engpässe in Militärmärkten, die Märkte blieben offen. In Europa große Warenverluste (Lilienthal über 360.000 Euro, eine belgische Delhaize-Filiale rund 100.000 Euro) und in Frankreich ein Angriff auf Kühlung von Blutkonserven, der rechtzeitig gestoppt wurde. Eine Gefahr für die Versorgung der Bevölkerung ist bisher nicht belegt. Das Risiko liegt eher bei falsch gekühlter Ware und bei Brandgefahr durch Heizbetrieb.
Behörden	USA: DCIS (Federführung), Army CID Cyber Field Office, US Cyber Command, Kontakt zu französischen Ermittlern; CISA, FBI, HHS, USDA, DOT (Factsheet). Frankreich: CERT-FR/ANSSI, Staatsanwaltschaft. Belgien: Föderalstaatsanwaltschaft, CCB. Deutschland: BSI (Warnung), Staatsanwaltschaft, Kripo Landshut.
Regulatorik	Die Commissaries unterliegen US-Bundesrecht, NIS2 gilt dort nicht. Für DACH: Große Lebensmittelhändler und Lebensmittelproduzenten fallen unter NIS2 (Sektor Produktion, Verarbeitung und Vertrieb von Lebensmitteln), mit Meldepflicht (Frühwarnung binnen 24 Stunden). Einzelne Märkte und kleine Betreiber liegen meist unter den Schwellen. Der CRA verpflichtet Hersteller vernetzter Steuerungen künftig zu Sicherheitsupdates und Schwachstellenmeldungen.

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

• Direkt aus dem Internet erreichbare Web-Oberfläche der Kältesteuerung mit Standard- oder schwachen Zugangsdaten (hoch): CISA nennt schwache Konfigurationen, CERT-FR fordert ausdrücklich, Standardpasswörter zu ändern. Forescout zählt Tausende exponierte Systeme. Für die US-Basen ist nicht belegt, dass sie exponiert waren.

• Ausnutzung bekannter Schwachstellen in alter Firmware (u. a. von Claroty gemeldete Lücken in Danfoss AK-SM 800A und Copeland XWEB Pro, z. B. Authentifizierungsumgehung) (hoch): CISA nennt Umgehung der Authentifizierung und Code-Ausführung. Danfoss bestätigt viele veraltete Geräte in Frankreich, für alte Hardware gibt es keine Patches. Ob diese Lücken tatsächlich ausgenutzt wurden, ist nicht belegt.

• Kompromittierter Fernwartungszugang des Kältedienstleisters (Supply-Chain-Weg) (mittel): Ein betroffener Markt in Wetter-Volmarstein sagt, der Angriff habe eigentlich der Fernwartungsfirma gegolten. CERT-FR erwähnt Datenverbindungen zu Kältedienstleistern. Ein Beleg für die USA fehlt.

• Eindringen über das IT-Netz des Betreibers und Lateral Movement zur Steuerung (gering): Die Gleichzeitigkeit an vielen unabhängigen Betreibern spricht eher für Massenscans auf exponierte Geräte als für gezielte Einbrüche in einzelne Firmennetze.

Zeitleiste

26.08.2026 Fort Huachuca meldet, alle Gefriertruhen seien über Nacht in den Abtaumodus gegangen (Blog Signal and Silence nennt den 27.08.) – bestätigt [https://www.militarytimes.com/pentagon/2026/10/29/pentagon-treating-military-base-freezer-malfunctions-as-suspected-cyberattack-officials-say/]

28.08.2026 DoD bestätigt eine „possible refrigeration disruption“ in einigen Commissaries – bestätigt

[https://militarytimes.com/news/your-military/2026/08/28/dod-confirms-refrigeration-disruption-at-military-commissaries/]

01.09.2026 Army CID ermittelt zu den Ausfällen – bestätigt
[https://www.stripes.com/theaters/us/2026-09-01/army-cid-investigates-commissary-refrigerator-outages-22721718.html]

Ende 09.2026 Kühlausfälle in vier Commissaries in Deutschland und England; laut DeCA Verschleiß und Ersatzteilmangel, ohne Zusammenhang mit den US-Fällen – bestätigt
[https://www.stripes.com/theaters/europe/2026-09-30/freezer-outages-europe-commissaries-23013166.html]

11./12.10.2026 Angriffe auf Kältesteuerungen in Hunderten französischen Supermärkten – bestätigt [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

12.10.2026 (Update 13. und 16.10.) CERT-FR-Alerte zu Danfoss AK-SC/AK-SM, Copeland und Dixell XWEB – bestätigt [https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

22.10.2026 Forescout: 6.017 exponierte IPs in 99 Ländern – bestätigt
[https://www.forescout.com/blog/cold-chain-open-control-exposed-refrigeration-systems-reveal-global-risk/]

29.10.2026 Reuters: Pentagon behandelt Ausfälle als mutmaßlichen Hack; Nextgov: Iran-Verdacht – berichtet
[https://www.nextgov.com/cybersecurity/2026/10/officials-suspect-iran-series-cyberattacks-military-base-freezers/416934/]

02.11.2026 Zweite Welle in rund einem Dutzend Ländern, u. a. Belgien (mind. 76 Geschäfte) und Deutschland (Reisbach bis 50 °C, Raesfeld, Wuppertal, Wetter-Volmarstein, Lilienthal) – bestätigt
[https://www.zdfheute.de/politik/deutschland/cyberangriff-supermaerkte-nrw-bayern-temperatur-100.html]

02./03.11.2026 Belgische Föderalstaatsanwaltschaft ermittelt; Kripo Landshut ermittelt wegen Datenausspähung und Datenveränderung – bestätigt
[https://www.vrt.be/vrtnws/en/2026/11/03/belgian-prosecutors-launch-investigation-into-supermarket-cybera/]

05.11.2026 Gemeinsames Factsheet von CISA, FBI, HHS, USDA und DOT – bestätigt [https://www.cisa.gov/resources-tools/resources/us-government-partners-urge-hardening-industrial-refrigeration-and-cold-chain-monitoring-systems]

Vergleichsfälle

• Angriffe auf Kühlsteuerungen in 16 russischen Supermärkten, von Danfoss dokumentiert (2022): Das Muster war schon Jahre vorher bekannt, nur hat es kaum jemand ernst genommen. [https://www.pcgameshardware.de/Sicherheit-Thema-229955/News/hacker-supermarkt-kuehltruhen-50-grad-danfoss-warnung-2025-1556696/]

• Frankreich: Hunderte Supermärkte mit manipulierter Kühlung (2026): Ein Reset hilft nur kurz, wenn das Gerät danach wieder ungeschützt online ist.
[https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-012/]

Begriffe einfach erklärt

OT: Operational Technology, also die Technik, die physische Dinge steuert, hier die Kühlung.

Kältesteuerung: Kleiner Computer, der Temperaturen, Abtauzyklen und Alarme einer Kühlanlage regelt.

Abtaumodus: Normaler Betriebszustand, in dem das Gerät kurz heizt, um Eis zu entfernen; bleibt er dauerhaft an, taut alles auf.

Fernwartung: Zugriff des Kältetechnikers aus der Ferne über das Internet.

Commissary: Supermarkt auf einer US-Militärbasis für Soldaten und ihre Familien.

Firmware: Die fest eingebaute Software eines Geräts, die Updates braucht wie ein Handy.

Früherer Stand: Erstmeldung (29.10.2026 15:33)

Wissen 48 % · wahrscheinlich 19 % · nicht bekannt 33 %
Ende August 2026 sind in mehreren Commissaries auf US-Militärbasen Kühl- und Gefrieranlagen in den Abtaumodus gegangen, die Ware verdarb. Laut Reuters (29.10.2026, vier anonyme Beamte) behandelt das Pentagon die Ausfälle inzwischen als mutmaßlichen Hack, eine Einheit des Cyber Command ermittelt mit, außerdem gibt es Kontakt zu französischen Behörden. Ursache, Zugangsweg, Täter und eine Verbindung zu Danfoss oder zu den im August

veröffentlichten Schwachstellen sind nicht bestätigt.

Früherer Stand: Nach 24 Stunden (30.10.2026 15:37)

Wissen 51 % · wahrscheinlich 17 % · nicht bekannt 32 %

Ende August 2026 gingen in mindestens sechs Commissaries auf US-Militärbasen Gefriertruhen in den Abtaumodus, die Ware verdarb. Laut Reuters (29.10.2026, vier anonyme Beamte) behandelt das Pentagon das inzwischen als mutmaßlichen Hack, eine Einheit des US Cyber Command ist beteiligt und die Ermittler sprechen mit Frankreich, wo im Oktober Kühlsteuerungen in Hunderten Supermärkten manipuliert wurden. Ursache, Initial Access, Täter und eingesetzte Steuerungstechnik sind öffentlich nicht bestätigt, nur für einen einzigen Standort (NAF El Centro) nennen Unterlagen eine Danfoss-Steuerung.

Früherer Stand: Nach 72 Stunden (01.11.2026 15:42)

Wissen 49 % · wahrscheinlich 18 % · nicht bekannt 33 %

Ende August 2026 fielen in mindestens sechs Commissaries auf US-Militärbasen Kühl- und Gefriergeräte aus, weil sie über Nacht in den Abtaumodus gingen. Die Ware verdarb. Laut Reuters (29.10.2026, vier anonyme Beamte) behandelt das Pentagon das als mutmaßlichen Hack, Cyber Command und mehrere militärische Ermittlungsbehörden sind beteiligt und stehen in Kontakt mit Frankreich. Ursache, Initial Access, eingesetzte Steuerungen und Täter sind offiziell nicht bestätigt; einen Iran-Bezug melden nur zwei anonyme Quellen über Nextgov.

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