CHUBB®

November 2026

BREAKING ALERT:

Chubb Vulnerability Alert System:

"Targeted Attacks Against Remote Refrigeration System Controllers"

Chubb provides alerts to keep our policyholders informed of risks that may affect their organizations. Chubb has noted multiple compromises of remote controllers for Danfoss AK-SM and AK-SC series refrigeration systems, as well as Copeland XWEB and Dixell XWEB systems. Other internet-facing refrigeration systems may also be affected.

Chubb recommends the following best practices to reduce the likelihood of falling victim to targeted attacks:

Identify exposed controllers: Inventory Danfoss AK-SM/AK-SC, Copeland/Dixell XWEB and other refrigeration management systems. Identify internet-exposed interfaces, including those on independently managed cellular connections.

Remove direct internet access: Disable **internet**-facing management interfaces and port forwarding. Require secure VPN or equivalent protected access for authorized maintenance providers.

Patch or replace vulnerable equipment: Apply current manufacturer firmware and security updates. Prioritize legacy and end-of-life controllers that cannot be patched.

Harden remote access: Change default/shared credentials, enforce unique accounts and MFA where supported, enable Danfoss Strict security mode, and restrict vendor privileges.

Validate configurations and monitor: Review temperature thresholds, defrost schedules, alarms and configuration-change logs. Establish independent temperature monitoring and a recovery procedure for compromised controllers.

If compromised: In addition to removing internet exposure, restart the affected Danfoss device. Reconfigure the equipment fully before returning it to service. A factory reset alone is insufficient for EOL devices. Without a security patch or network isolation, the device will very likely be re-compromised immediately.

Additional guidance on Danfoss security advisories can be found here.

Chubb's Cyber Risk Advisory Team is available to answer your questions and help mitigate cyber exposures like the one described above. To request advisory services, please click here.

For additional information, please contact cyber@chubb.com. You may also use Chubb's interactive tool Chubb Cyber Index® to access additional resources to help evaluate and address cyber risks your business may face.

Click here to learn more about Chubb's Cyber Services.

Chubb's cyber insurance policyholders are monitored using non-intrusive outside web scanning methods. While these methods vary and are subject to change, the insights generated are typically viewable in cybersecurity rating company reports, such as those provided by BitSight and Security Scorecard, which all Chubb cyber policyholders have complimentary access to review. For more information about vulnerability alerts and our scanning technology or to sign up, contact Chubb's Cyber Global Risk Advisors at cyber@chubb.com . Chubb makes no representations or warranties around these continuous monitoring efforts, and cannot reasonably alert all policyholders about all observed vulnerabilities. For more thorough service, consider speaking with a Managed Security Service Provider.

All content in this material is for general information purposes only. It does not constitute personal advice or a recommendation to any individual or business of any product or service. Please refer to the policy documentation issued for full terms and conditions of coverage.

All Cyber Services are subject to change. Changes to the service offerings will be displayed on the local Cyber Services web form. Policyholders are responsible for reviewing the specific terms and conditions of each Cyber Service provider to ensure eligibility and remain informed regarding any changes. The complimentary cost is applicable only to policyholders who are net new subscribers/customers to the respective services.

The services referenced are provided by a third-party vendor not affiliated with Chubb. The fact that offers and potential discounts may be made available by the third-party vendor is not an indication that insurance coverage is available under any Chubb policy for any particular incident. Discounts on products and services offered by this vendor are available only to Chubb policyholders with current in-force policies and are subject to applicable insurance laws. For products and services provided, the policyholder and third-party vendor would enter into a vendor relationship directly. Chubb will not be involved in the policyholder's decision to purchase services and has no responsibility for services that may be provided

Chubb European Group SE (CEG). Operating in the UK through a branch based at 40 Leadenhall Street, London EC3A 2BJ. Risks falling within the European Economic Area are underwritten by CEG which is governed by the provisions of the French insurance code. Registered company number: 450 327 374 RCS Nanterre. Registered office: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, France. Fully paid share capital of €896,176,662.