14.10.2026

Wichtige Sicherheitsinformation zu Fernzugriffen auf CAREL-Überwachungssysteme

Sehr geehrte Geschäftspartner,

nationale Cybersicherheitsbehörden in Frankreich (CERT-FR) und Italien (ACN / CSIRT Italia) haben jüngst über Cyberangriffe auf Fernüberwachungs- und Fernsteuerungssysteme von Kälteanlagen informiert. Nach den vorliegenden Erkenntnissen betrafen die Vorfälle vor allem ältere Installationen, Systeme mit direkter Internetanbindung sowie unzureichend abgesicherte Fernzugänge.

Obwohl bislang keine Sicherheitslücke in CAREL-Produkten im Zusammenhang mit diesen Vorfällen festgestellt wurde, empfehlen wir vorsorglich, alle Installationen mit internetfähigen CAREL-Systemen kurzfristig zu überprüfen.

Unsere Empfehlungen

1. Prüfen Sie die Erreichbarkeit Ihres CAREL-Supervisors

Bitte lassen Sie durch Ihren Installateur oder Servicepartner prüfen, ob Ihr CAREL-Supervisor aus dem Internet erreichbar ist.

Als sicher gelten ausschließlich folgende Konfigurationen:

- Das System ist nicht mit dem Internet verbunden.
- Der Fernzugriff erfolgt ausschließlich über eine gesicherte VPN-Verbindung.

Eine direkte Erreichbarkeit aus dem Internet, beispielsweise über Portweiterleitungen (Port Forwarding), wird ausdrücklich nicht empfohlen.

2. Bei Unsicherheit oder direkter Erreichbarkeit sofort handeln

Sollte der Supervisor direkt aus dem Internet erreichbar sein oder keine eindeutige Aussage zur Konfiguration möglich sein, empfehlen wir, die Internetverbindung vorsorglich zu deaktivieren, bis die Installation überprüft wurde.

Die Kommunikation zwischen Supervisor und den angeschlossenen Feldgeräten kann dabei unverändert bestehen bleiben.

3. Überprüfen Sie Betriebsparameter und Ereignisprotokolle

Bitte kontrollieren Sie insbesondere:

- Temperaturwerte und Sollwerte
- Dauer und Häufigkeit von Abtauzyklen
- Alarmgrenzen und Alarmempfänger
- Ereignis- und Benutzerprotokolle

Achten Sie auf ungewöhnliche Änderungen, wie beispielsweise:

- ungewöhnlich lange Abtauzyklen
- unerklärliche Temperaturabweichungen
- unbekannte Benutzeraktivitäten
- deaktivierte Alarmfunktionen

4. Sicheren Fernzugriff sicherstellen

Eine Wiederanbindung an das Internet sollte erst erfolgen, nachdem Ihr Installateur bestätigt hat, dass der Remote-Zugriff ausschließlich über gesicherte Verbindungen, beispielsweise VPN-Lösungen, erfolgt und die empfohlenen Maßnahmen umgesetzt wurden.

5. Softwarestand prüfen

Zusätzlich empfehlen wir, die installierte Softwareversion Ihres CAREL-Supervisors zu überprüfen und gegebenenfalls auf die aktuell freigegebene Version zu aktualisieren. Ihr Installations- oder Servicepartner unterstützt Sie hierbei gerne.

Meldung von Auffälligkeiten

Falls Sie ungewöhnliche Systemereignisse oder verdächtige Aktivitäten feststellen, dokumentieren Sie diese bitte durch Logdateien oder Screenshots und informieren Sie umgehend Ihren CAREL-Ansprechpartner.

Ihr Beitrag zur Systemsicherheit

Wir bitten Sie, die genannten Prüfungen zeitnah einzuleiten und gegebenenfalls Ihre Installations- bzw. Wartungspartner einzubinden. Durch proaktive Maßnahmen können potenzielle Risiken frühzeitig erkannt und vermieden werden.

Wir bitte um Bestätigung des Erhalts dieses Schreibens und eine zeitnahe Umsetzung der Empfehlungen.

Für Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

CAREL Deutschland GmbH

14.10.2026

Important Security Information Regarding Remote Access to CAREL Monitoring Systems

Dear Business Partner,

The national cybersecurity authorities in France (**CERT-FR**) and Italy (**ACN / CSIRT Italia**) have recently reported cyberattacks targeting remote monitoring and remote control systems used in refrigeration installations. According to the information available, these incidents primarily affected older installations, systems with direct internet connectivity, and inadequately secured remote access configurations.

Although no security vulnerability in CAREL products has been identified in connection with these incidents, we recommend, as a precautionary measure, that all installations using internet-enabled CAREL systems be reviewed without delay.

Our Recommendations

1. Verify the Accessibility of Your CAREL Supervisor

Please ask your installer or service partner to verify whether your CAREL Supervisor is accessible from the internet.

Only the following configurations should be considered secure:

- The system is not connected to the internet.
- Remote access is provided exclusively through a secure VPN connection.

Direct accessibility from the internet, for example through port forwarding, is strongly discouraged.

2. Take Immediate Action if in Doubt or if Direct Accessibility Exists

If the Supervisor is directly accessible from the internet, or if the system configuration cannot be clearly confirmed, we recommend disconnecting the internet connection as a precaution until the installation has been inspected.

Communication between the Supervisor and connected field devices can remain fully operational during this period.

3. Review Operating Parameters and Event Logs

Please pay particular attention to:

- Temperature readings and setpoints
- Defrost cycle duration and frequency
- Alarm thresholds and alarm recipients
- Event and user logs

Look for unusual changes, such as:

- Unusually long defrost cycles
- Unexplained temperature deviations
- Unknown user activities
- Disabled alarm functions

4. Ensure Secure Remote Access

The system should only be reconnected to the internet after your installer has confirmed that remote access is provided exclusively through secure connections, such as VPN solutions, and that all recommended security measures have been implemented.

5. Verify the Software Version

We also recommend checking the installed software version of your CAREL Supervisor and upgrading to the latest approved release if necessary. Your installation or service partner will be pleased to assist you.

Reporting Suspicious Activity

If you detect any unusual system events or suspicious activities, please document them using log files and/or screenshots and notify your CAREL contact person immediately.

Your Contribution to System Security

We kindly ask you to initiate the above checks promptly and, where appropriate, involve your installation and maintenance partners. By taking proactive measures, potential risks can be identified and mitigated at an early stage.

We would appreciate your confirmation of receipt of this letter and the timely implementation of the recommendations outlined above.

Should you have any questions, please do not hesitate to contact us.

Yours sincerely,

CAREL Deutschland GmbH