Produktmitteilung

Sicherheitshinweis für XWEB-Überwachungssysteme

Sehr geehrte Kundin, sehr geehrter Kunde, seit über 30 Jahren ist Copeland Controls ein vertrauenswürdiger Marktführer in den Bereichen Kältetechnik und HLK und liefert zuverlässige, hochwertige Produkte, die Branchenstandards setzen. Unser Vermächtnis basiert auf Exzellenz, gestützt durch strenge Tests und ein unerschütterliches Bekenntnis zu Zuverlässigkeit und Leistung. Die XWEB-Überwachungseinheiten von Copeland Controls leisten seit über zwei Jahrzehnten zuverlässige Dienste für Kunden in wichtigen Märkten. In dieser Zeit haben sich die technologischen und sicherheitstechnischen Anforderungen erheblich weiterentwickelt, und wir setzen uns dafür ein, dass unsere Produkte den heutigen Standards entsprechen. Die Gewährleistung von Sicherheit, Qualität und Schutz unserer Produkte ist ein wesentlicher Bestandteil unseres Handelns. Wir arbeiten aktiv mit der globalen Cybersicherheits-Community zusammen und ermutigen externe Experten, potenzielle Schwachstellen über unsere dafür vorgesehenen Prozesse zu melden. Dies fördert Transparenz, Vertrauen und kontinuierliche Verbesserung.

Uns sind Berichte über eine Cybersicherheitslücke bekannt, die sowohl die nicht mehr weitergeführte, auslaufende XWEB EVO-Plattform als auch XWEB PRO-Systeme betrifft, auf denen veraltete Softwareversionen laufen. Wir haben das Problem identifiziert und geben die folgenden Empfehlungen, um Kunden bei der Absicherung ihrer Systeme zu unterstützen.

Empfehlungen für die sichere Nutzung von XWEB-Supervisoren

Zusammenfassung

Entfernen Sie alle XWEB-Geräte unverzüglich aus dem öffentlichen Internet, überprüfen Sie anschließend das lokale Netzwerk auf verdächtige Aktivitäten und setzen Sie die Geräte gegebenenfalls zurück.

Dieser Hinweis listet zusätzliche Maßnahmen auf, die zur Verringerung des mit XWEB-Supervisoren verbundenen Cybersicherheitsrisikos umgesetzt werden können, und erläutert, wie ein Gerät wiederhergestellt wird, auf das möglicherweise unbefugt zugegriffen wurde.

1. **Planen Sie Ihre Migration**. XWEB EVO hat das Ende des Supports erreicht und erhält keine Sicherheitspatches mehr; XWEB PRO ist die unterstützte Plattform. Auch bei PRO sollten Sie das Gerät nicht dem Internet aussetzen
2. **Beseitigen Sie die Internetpräsenz.** Stellen Sie sicher, dass von außerhalb Ihres lokalen Netzwerks kein Zugriff auf XWEB möglich ist (siehe *„Sofortige Maßnahmen zur Risikominderung“*).
3. **Überprüfen und stellen Sie das Gerät wieder her.** Befolgen Sie die Schritt-für-Schritt-Anleitung und arbeiten Sie dabei ausschließlich aus dem lokalen Netzwerk heraus.

Sofortmaßnahmen zur Risikominderung

Wenden Sie diese Maßnahmen auf jedes XWEB an, unabhängig davon, ob Sie einen unbefugten Zugriff vermuten oder nicht.

- **Entfernen Sie XWEB aus dem öffentlichen Internet.** Keine Portweiterleitung, keine DMZ und keine direkte öffentliche IP-Adresse.
- **Beschränken Sie den physischen Zugriff** ausschließlich auf autorisiertes Personal (beschränken Sie beispielsweise den Zutritt zu Geräteräumen und nutzen Sie nach Möglichkeit einen Schlüsselzugang).
- **Verwenden Sie** für den Fernzugriff **einen VPN-Dienst**, damit das XWEB-Gerät nur über einen eingeschränkten und verschlüsselten Tunnel erreicht werden kann.

Copeland Controls S.r.l. | Z.I. Via dell’Industria, 27
32016 Alpago (BL) ITALIEN – copeland.com – dixell@copeland.com
Weitere Informationen finden Sie unter **copeland.com**
©2026 Copeland LP

Empfehlungen von Copeland Controls

Befolgen Sie alle Anweisungen und Spezifikationen im Gerätehandbuch und wenden Sie bewährte Sicherheitspraktiken an, unter anderem:

- das Steuerungssystem niemals dem offenen Internet aussetzen;
- Konfigurieren Sie Ihre Firewall so, dass der Zugriff auf Verwaltungsprotokolle wie SSH eingeschränkt wird;
- Konfigurieren Sie Ihr Netzwerk so, dass die ein- und ausgehende Kommunikation zum und vom Steuerungssystem eingeschränkt wird;
- Aktualisieren Sie die Passwörter der Standardkonten und stellen Sie sicher, dass die Passwörter den branchenüblichen Best Practices entsprechen;
- Konfigurieren und Aktivieren von HTTPS für den webbasierten Datenverkehr, ohne die Weboberfläche des Controllers dem offenen Internet auszusetzen.

So überprüfen und wiederherstellen Sie ein potenziell kompromittiertes XWEB

Stellen Sie eine Verbindung zum XWEB ausschließlich über das lokale Netzwerk her und führen Sie die folgenden Schritte der Reihe nach durch.

Bevor Sie beginnen

- **Isolieren Sie das Gerät.** Entfernen Sie alle Portweiterleitungen oder DMZ-Regeln, die auf das XWEB verweisen, oder trennen Sie die WAN-Verbindung des Routers, bevor Sie beginnen.
- **Halten Sie Ihre Befunde fest.** Erstellen Sie Screenshots der Benutzerliste, der Profile und der Systemeinstellungen, bevor Sie Änderungen vornehmen. Der Copeland-Support benötigt diese möglicherweise, ebenso wie für einen etwaigen Vorfallbericht.

Vorgehensweise

1. **Melden Sie sich mit Ihrem Administrator-Passwort an.**
    - Falls das Passwort geändert wurde und Sie sich nicht anmelden können, wenden Sie sich bitte rund um die Uhr an den technischen Support von Copeland unterColdChain.TechnicalServices@copeland.com und bitten Sie um Anweisungen zum Erhalt eines temporären Zugangspassworts.
    - Der Support benötigt das aktuelle XWEB-Datum und die MAC-Adresse, die auf der XWEB-Anmeldeseite angezeigt wird. Drücken Sie auf der Anmeldeseite **STRG+ALT,** um die MAC-Adresse anzuzeigen.
2. **Stellen Sie Ihr letztes Backup wieder her.** Stellen Sie nach der Anmeldung das aktuellste Backup wieder her, indem Sie Folgendes auswählen:
    - System
    - Geräte, Layout, Tools, Benutzer
    - Stellen Sie sicher, dass die Sicherung *vor* dem vermuteten unbefugten Zugriff erstellt wurde.
3. **Falls Sie keine Sicherung haben, überprüfen Sie die Benutzer und Profile.** Vergewissern Sie sich, dass die Benutzerliste Ihren Erwartungen entspricht, und entfernen Sie alle Benutzer oder Profile, die Sie nicht erkennen.
4. **Ändern Sie alle Benutzerkennwörter.** Jedes Kennwort muss folgende Mindestanforderungen erfüllen:
    - Mindestens 8 Zeichen
    - Mindestens eine Ziffer
    - Mindestens ein Großbuchstabe
    - Mindestens ein Kleinbuchstabe
    - Darf den Benutzernamen nicht enthalten
    - Darf weder den Hostnamen noch den Systemnamen enthalten
    - Darf nicht aus einem einzigen sich wiederholenden Zeichen bestehen (z. B. aaaaaaaa)
    - *Empfohlen: 12 oder mehr Zeichen, mindestens ein Sonderzeichen und ein unterschiedliches Passwort für jedes Konto.*
5. **Aktualisieren Sie die Software.**
    - **XWEB PROs** Es wird dringend empfohlen, dass alle Kunden auf die neueste verfügbare Version,

©2026 Copeland LP

derzeit v.1.16.1, aktualisieren.
    - **XWEB EVOs** werden nicht mehr unterstützt. Es wird dringend empfohlen, dass alle Kunden auf eine unterstützte Plattform umsteigen.
    - Laden Sie die neueste Softwareversion für Ihr XWEB-Modell von der Copeland-Seite „System-Software-Update“ herunter und installieren Sie sie über **SYSTEM > Update > Updates**.
6. **Überprüfen Sie die Systemkonfiguration.** Stellen Sie sicher, dass alle genutzten Dienste korrekt eingerichtet sind, einschließlich der Netzwerkeinstellungen (Gateway und DNS) und der Mailserver-Einstellungen.
7. **Überprüfen Sie die Alarmverwaltung.**
    - Es sind Alarmkategorien vorhanden, die den Alarmvariablen der Geräte zugewiesen sind.
    - Bei Bedarf sind Alarmkategorien mit einer Stufe verknüpft, die E-Mail- oder SMS-Benachrichtigungen versendet oder Alarmrelais auslöst.
    - Die Empfänger für E-Mail- und SMS-Benachrichtigungen sind vorhanden und korrekt hinterlegt.
    - Lösen Sie einen Testalarm aus, um zu überprüfen, ob die Benachrichtigungen tatsächlich zugestellt werden.

8. **Stellen Sie die Geräteparameter aus Sicherungsdateien wieder her**, sofern vorhanden:
    1. Wählen Sie das Gerät unter **„GERÄTE“** aus.
    2. Öffnen Sie die Registerkarte **„Parameter**“.
    3. Klicken Sie auf **„Importieren“** und wählen Sie die Sicherungsdatei aus.
    4. Sobald die Parameterwerte geladen sind, klicken Sie auf **„Schreiben**“.
9. **Wenn Sie keine Parameter-Sicherungen haben,** wählen Sie jedes Gerät nacheinander aus, führen Sie ein **Auslesen** der Parameter durch und überprüfen Sie, ob diese für die Anwendung geeignet sind (Sollwerte, Alarmschwellen, Abtaueinstellungen).
10. **Erstellen Sie eine neue Sicherungskopie.** Erstellen Sie nach Abschluss der Überprüfungen und einer eventuellen Wiederherstellung stets eine neue Sicherungskopie und bewahren Sie eine Kopie außerhalb des Geräts auf.

Zusätzliche Empfehlungen zur Absicherung des Zugriffs

Diese Maßnahmen schließen die häufigsten Angriffspunkte ab, die über die oben genannten Grundlagen hinausgehen.

Fernzugriff

- **Nutzen Sie einen VPN-Dienst.** Wenden Sie sich an Ihre IT-Abteilung, um Unterstützung bei der Implementierung des von Ihrer Organisation genehmigten VPN-Dienstes zu erhalten

Netzwerk

- Platzieren Sie das XWEB in einem dedizierten Netzwerksegment (VLAN), das von den WLAN-Netzwerken für Büro, Kassensysteme und Gäste getrennt ist.
- Lassen Sie nur den ausgehenden Datenverkehr zu, den das XWEB benötigt (z. B. Mailserver, DNS, NTP und den Copeland-Update-Server), und blockieren Sie alles andere.
- Überprüfen Sie die Erreichbarkeit von außen: Versuchen Sie von einer Verbindung außerhalb des Standortnetzwerks aus – beispielsweise von einem Smartphone mit deaktiviertem WLAN – die öffentliche IP-Adresse des Standorts in einem Browser aufzurufen. Die Anmeldeseite des XWEB darf nicht angezeigt werden.

Konten und Passwörter

- Jeder Benutzer muss über ein eindeutiges, benanntes Konto verfügen; gemeinsam genutzte Konten sollten nicht zulässig sein.
- Weisen Sie jedem Konto das restriktivste Profil zu, das für die jeweilige Aufgabe geeignet ist, und beschränken Sie die Administratorrechte auf ein oder zwei Personen.
- Deaktivieren oder löschen Sie Konten, die nicht mehr benötigt werden, und überprüfen Sie die Benutzerliste mindestens einmal im Jahr.

©2026 Copeland LP

- Ändern Sie Passwörter nach jedem Besuch eines externen Dienstleisters, bei dem ein Konto mit erweiterten Rechten verwendet wurde.
- Verwenden Sie XWEB-Passwörter niemals anderweitig wieder und leiten Sie sie nicht vom Standort-, Speicher- oder Installateurnamen ab.

Überwachung und Datensicherung

- Sichern Sie die Systemkonfiguration und die Geräteparameter regelmäßig sowie nach jeder wesentlichen Änderung; bewahren Sie Kopien außerhalb des Geräts auf.
- Halten Sie die XWEB-Uhr synchronisiert (NTP), damit Aufzeichnungen und Protokolle genaue Zeitstempel enthalten.

Wenn Sie einen unbefugten Zugriff vermuten

- Trennen Sie das Gerät zunächst vom Netzwerk und stellen Sie es anschließend wieder her (siehe *„Bevor Sie beginnen*“).
- Überprüfen Sie die Produkttemperaturen direkt an den Gehäusen: Geänderte Sollwerte oder Alarmschwellen können die Lebensmittelsicherheit gefährden.
- Benachrichtigen Sie den technischen Support von Copeland sowie Ihr IT- oder Sicherheitsteam und, falls erforderlich, die zuständige Behörde (in den USA: CISA).

Planen Sie Ihre Migration zu XWEB PRO

XWEB EVO hat das Ende des Supports erreicht und erhält keine weiteren Software-Updates oder Sicherheitspatches mehr. Wir empfehlen Ihnen dringend, auf XWEB PRO umzusteigen, die aktuelle Plattform, die aktiv gepflegt und regelmäßig aktualisiert wird.

Technischer Support

Der technische Support von Copeland steht Ihnen rund um die Uhr unterColdChain.TechnicalServices@copeland.com zur Verfügung.

©2026 Copeland LP