Bulletin produit

Avis de sécurité relatif aux systèmes de supervision XWEB

Cher Client, depuis plus de 30 ans, Copeland Controls est un acteur de référence de la réfrigération et du génie climatique (HVAC), reconnu pour des produits fiables et de grande qualité qui font référence dans le secteur. Notre héritage repose sur une exigence d'excellence, portée par des essais rigoureux et un engagement constant en faveur de la fiabilité et de la performance. Depuis plus de vingt ans, les unités de supervision XWEB de Copeland Controls assurent un service fiable auprès de clients opérant sur des marchés essentiels. Au cours de cette période, les technologies et les exigences de sécurité ont considérablement évolué, et nous nous engageons à ce que nos produits répondent aux normes actuelles. Garantir la sûreté, la qualité et la sécurité de nos produits fait partie intégrante de chacune de nos actions. Nous collaborons activement avec la communauté internationale de la cybersécurité et encourageons les experts externes à signaler d'éventuelles vulnérabilités par l'intermédiaire de nos procédures dédiées. Cette démarche favorise la transparence, la confiance et l'amélioration continue.

Nous reconnaissons l'existence de la vulnérabilité identifiée sur une génération de contrôleurs XWEB EVO dont la commercialisation est arrêtée et qui est parvenue en fin de vie. Une enquête approfondie a été engagée ; les recommandations qui suivent permettent de remédier à cette vulnérabilité et de garantir la sécurité des systèmes de nos clients.

Recommandations pour une utilisation sûre des superviseurs XWEB

Synthèse

Retirez immédiatement toutes les unités XWEB EVO de l'Internet public, puis recherchez toute activité suspecte depuis le réseau local et restaurez les appareils si nécessaire.

Le présent avis énumère des mesures complémentaires permettant de réduire le risque de cybersécurité lié aux superviseurs XWEB EVO et explique comment remettre en état une unité ayant pu faire l'objet d'un accès non autorisé.

1. **Supprimez l'exposition à Internet.** Assurez-vous que les unités XWEB EVO ne sont pas accessibles depuis l'extérieur de votre réseau local (voir *Mesures immédiates de réduction des risques*).
2. **Vérifiez et restaurez l'unité.** Suivez la procédure pas à pas, en travaillant uniquement depuis le réseau local.
3. **Planifiez votre migration.** Le XWEB EVO a atteint sa fin de service (End of Service) et ne reçoit plus de correctifs de sécurité ; le XWEB PRO est la plateforme prise en charge. Le XWEB PRO lui-même ne doit pas être exposé à Internet.

Mesures immédiates de réduction des risques

Appliquez ces mesures à chaque XWEB EVO, que vous soupçonniez ou non un accès non autorisé.

- **Retirez les unités XWEB EVO de l'Internet public.** Aucune redirection de port, aucune DMZ et aucune adresse IP publique directe.
- **Restreignez l'accès physique** au seul personnel autorisé (par exemple, en limitant l'accès aux locaux techniques et en utilisant des serrures à clé lorsque c'est possible).
- **Utilisez un service VPN** pour l'accès à distance, afin que le XWEB ne soit joignable qu'au travers d'un tunnel chiffré et restreint.

Recommandations de Copeland Controls

Suivez l'ensemble des instructions et spécifications figurant dans le manuel de l'appareil et appliquez les bonnes pratiques de sécurité, notamment, sans que cette liste soit limitative :

- ne jamais exposer le système de régulation à l'Internet ouvert ;
- configurer votre pare-feu afin de restreindre l'accès aux protocoles d'administration, tels que SSH ;
- configurer votre réseau afin de restreindre les communications entrantes et sortantes du système de régulation ;
- modifier les mots de passe des comptes par défaut et veiller à ce que les mots de passe soient conformes aux bonnes pratiques du secteur ;
- configurer et activer HTTPS pour le trafic web, sans exposer l'interface web du contrôleur à l'Internet ouvert.

Copeland Controls S.r.l. | Z.I. Via dell'Industria, 27
32016 Alpago (BL) ITALIE - copeland.com - dixell@copeland.com
Pour en savoir plus, rendez-vous sur **copeland.com**
©2026 Copeland LP

COPELAND

Comment vérifier et restaurer un XWEB EVO potentiellement compromis

Connectez-vous au XWEB uniquement depuis le réseau local et suivez les étapes ci-dessous dans l'ordre.

Avant de commencer

- **Isolez l'unité.** Supprimez toute règle de redirection de port ou de DMZ pointant vers le XWEB, ou déconnectez la liaison WAN du routeur.
- **Consignez vos constats.** Effectuez des captures d'écran de la liste des utilisateurs, des profils et des paramètres système avant toute modification. Le support technique de Copeland pourra en avoir besoin, de même que tout rapport d'incident.

Procédure

1. **Connectez-vous avec votre mot de passe administrateur.**
    - Si le mot de passe a été modifié et que vous ne parvenez pas à vous connecter, contactez le support technique de Copeland, disponible 24 h/24 et 7 j/7, à l'adresse ColdChain.TechnicalServices@copeland.com et demandez la marche à suivre pour obtenir un mot de passe d'accès temporaire.
    - Le support technique de Copeland aura besoin de la date actuelle du XWEB EVO et de l'adresse MAC affichée sur la page de connexion du XWEB. Appuyez sur **CTRL+ALT** sur la page de connexion pour afficher l'adresse MAC.
2. **Restaurez votre dernière sauvegarde.** Une fois connecté, restaurez la sauvegarde la plus récente en sélectionnant :
    - Système
    - Régulateurs, Layout, Outils, Utilisateurs
    - Assurez-vous que la sauvegarde a été créée *avant* l'accès non autorisé présumé.
3. **En l'absence de sauvegarde, vérifiez les utilisateurs et les profils.** Contrôlez que la liste des utilisateurs correspond à ce que vous attendez et supprimez tout utilisateur ou profil que vous ne reconnaissez pas.
4. **Modifiez les mots de passe de tous les utilisateurs.** Chaque mot de passe doit respecter les exigences minimales suivantes :
    - Au moins 8 caractères
    - Au moins un chiffre
    - Au moins une lettre majuscule
    - Au moins une lettre minuscule
    - Ne pas contenir le nom d'utilisateur
    - Ne pas contenir le nom d'hôte ni le nom du système
    - Ne pas être constitué d'un seul caractère répété (par exemple, aaaaaaaa)
    - *Recommandé : 12 caractères ou plus, au moins un symbole et un mot de passe différent pour chaque compte.*
5. **Mettez à jour le logiciel.** Les unités XWEB EVO ne sont plus prises en charge. Il est vivement recommandé à tous les clients de migrer vers une plateforme prise en charge. Dans l'intervalle, téléchargez la dernière version logicielle correspondant à votre modèle de XWEB EVO depuis la page Copeland System Software Update et installez-la depuis **Système > Mises à jour > Mise à jour**.
6. **Vérifiez la configuration du système.** Contrôlez que chaque service utilisé est correctement paramétré, notamment les paramètres réseau (passerelle et DNS) et ceux du serveur de messagerie.
7. **Vérifiez la gestion des alarmes.**
    - Des catégories d'alarme existent et sont affectées aux variables d'alarme des appareils.
    - Le cas échéant, les catégories d'alarme sont associées à un niveau qui déclenche l'envoi de notifications par e-mail ou SMS, ou l'activation de relais d'alarme.
    - Les destinataires des notifications par e-mail et SMS sont renseignés et corrects.
    - Déclenchez une alarme de test pour vérifier que les notifications sont effectivement reçues.
8. **Restaurez les paramètres des appareils à partir des fichiers de sauvegarde**, si vous en disposez :
    - Sélectionnez l'appareil dans le menu **Régulateurs**.
    - Ouvrez l'onglet **Paramètres**.
    - Cliquez sur **Importer** et sélectionnez le fichier de sauvegarde.
    - Une fois les valeurs des paramètres chargées, cliquez sur **Écriture**.
9. **En l'absence de sauvegarde des paramètres,** sélectionnez successivement chaque appareil, cliquez sur **Lecture** pour lire ses paramètres et vérifiez qu'ils sont adaptés à l'application (consignes, seuils d'alarme, paramètres de dégivrage).
10. **Créez une nouvelle sauvegarde.** Une fois les vérifications et l'éventuelle restauration terminées, créez systématiquement une nouvelle sauvegarde et conservez-en une copie hors de l'unité.

Copeland Controls S.r.l. | Z.I. Via dell'Industria, 27
32016 Alpago (BL) ITALIE - copeland.com - dixell@copeland.com
Pour en savoir plus, rendez-vous sur **copeland.com**
©2026 Copeland LP

Recommandations complémentaires pour sécuriser l'accès

Ces mesures ferment les points d'entrée les plus courants, au-delà des mesures de base décrites ci-dessus.

Accès à distance

- **Utilisez un service VPN.** Consultez votre service informatique pour mettre en œuvre le service VPN approuvé par votre organisation.

Réseau

- Placez le XWEB sur un segment réseau dédié (VLAN), distinct des réseaux bureautiques, des réseaux des points de vente et des réseaux Wi-Fi invités.
- N'autorisez que le trafic sortant nécessaire au XWEB (par exemple, serveur de messagerie, DNS, NTP et serveur de mises à jour Copeland) et bloquez tout le reste.
- Vérifiez l'exposition depuis l'extérieur : à partir d'une connexion extérieure au réseau du site, par exemple un téléphone dont le Wi-Fi est désactivé, saisissez l'adresse IP publique du site dans un navigateur. La page de connexion du XWEB ne doit pas s'afficher.

Comptes et mots de passe

- Attribuez à chaque utilisateur un compte nominatif unique et n'autorisez pas les comptes partagés.
- Attribuez à chaque compte le profil le plus restrictif compatible avec sa fonction et limitez les droits d'administrateur à une ou deux personnes.
- Désactivez ou supprimez les comptes devenus inutiles et passez en revue la liste des utilisateurs au moins une fois par an.
- Modifiez les mots de passe après toute intervention d'un prestataire externe ayant utilisé un compte à privilèges.
- Ne réutilisez jamais les mots de passe du XWEB ailleurs et ne les construisez pas à partir du nom du site, du magasin ou de l'installateur.

Surveillance et sauvegardes

- Sauvegardez la configuration du système et les paramètres des appareils selon un calendrier régulier et après chaque modification importante ; conservez des copies hors de l'unité.
- Maintenez l'horloge du XWEB synchronisée (NTP) afin que les enregistrements et les journaux soient correctement horodatés.

En cas de suspicion d'accès non autorisé

- Isolez d'abord l'unité, puis remettez-la en état (voir *Comment vérifier et restaurer un XWEB EVO potentiellement compromis*).
- Vérifiez directement les températures des produits dans les meubles frigorifiques : des consignes ou des seuils d'alarme modifiés peuvent compromettre la sécurité sanitaire des aliments.
- Informez le support technique de Copeland ainsi que votre service informatique ou de sécurité et, le cas échéant, l'autorité compétente (aux États-Unis, la CISA).

Planifiez votre migration vers le XWEB PRO

Le XWEB EVO a atteint sa fin de service et ne recevra plus aucune mise à jour logicielle ni aucun correctif de sécurité. Nous recommandons vivement de migrer vers le XWEB PRO, la plateforme actuelle, activement maintenue et régulièrement mise à jour.

Support technique

Le support technique de Copeland est disponible 24 h/24 et 7 j/7 à l'adresse ColdChain.TechnicalServices@copeland.com.

Copeland Controls S.r.l. | Z.I. Via dell'Industria, 27
32016 Alpago (BL) ITALIE - copeland.com - dixell@copeland.com
Pour en savoir plus, rendez-vous sur **copeland.com**
©2026 Copeland LP

DIXELL FRANCE

Sécurité des superviseurs XWEB en France
Compléments au bulletin Copeland d'octobre 2026

En octobre 2026, Copeland a publié un bulletin produit consacré à la sécurité des superviseurs XWEB. Ses recommandations s'adressent à l'ensemble des utilisateurs, dans tous les pays.

Le présent document les complète par des informations propres au contexte français et par les modalités pratiques de leur mise en œuvre sur les XWEB PRO et XWEB EVO. Il s'ajoute au bulletin de Copeland qui fait référence et ne s'y substitue pas.

1. Interlocuteurs en France

Pour toute question relative à l'application de ces recommandations, Dixell France est votre interlocuteur en français. Les coordonnées sont en pied de page de ce document.

Le support technique de Copeland, joignable 24h/24 et 7j/7 à l'adresse ColdChain.TechnicalServices@copeland.com, répond en anglais.

Le bulletin de Copeland cite, pour les États-Unis, l'agence fédérale CISA. En France, l'autorité compétente en matière de sécurité des systèmes d'information est l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui publie ses avis et alertes de sécurité par l'intermédiaire du CERT-FR (cert.ssi.gouv.fr).

2. Mettre à jour le superviseur

Avant toute mise à jour

Relevez la version installée et réalisez une sauvegarde complète de la configuration, toutes les sections étant cochées : menu Système > Sauvegarde, sur le XWEB PRO comme sur le XWEB EVO.

Attention cette sauvegarde concerne que le paramétrage du XWEB mais n'archive ni les données historiques de fonctionnement, ni les paramètres des régulateurs.

Planifiez l'intervention en dehors des heures d'exploitation : le superviseur redémarre et l'enregistrement des températures est interrompu pendant quelques minutes.

Mise à jour du XWEB PRO

1. Connectez-vous au XWEB avec un compte administrateur.
2. Relevez la version actuelle du firmware.
3. Si le XWEB dispose d'un accès Internet, ouvrez le menu Système > Mise à jour et cliquez sur Réseau : le superviseur télécharge la mise à jour directement depuis les serveurs de Copeland.
4. Sans accès Internet, téléchargez le fichier correspondant à votre modèle sur la page de mise à jour logicielle de Copeland, puis chargez-le depuis le même menu Mise à jour.
5. Laissez le XWEB redémarrer sans couper son alimentation.
6. Reconnectez-vous et vérifiez que la nouvelle version s'affiche et que l'acquisition des données a repris.

Mise à jour du XWEB EVO

Le XWEB EVO a atteint sa fin de service et ne reçoit plus de correctif de sécurité. Dans l'attente de sa migration vers le XWEB PRO, installez la dernière version logicielle disponible pour votre modèle depuis le menu Système > Mises à jour, bouton Mise à jour. Trois modes sont proposés : Réseau (téléchargement par Internet), USB (clé USB branchée sur le XWEB) et Téléchargement (fichier envoyé depuis le navigateur, après téléchargement sur la page de mise à jour logicielle de Copeland). Les précautions décrites ci-dessus s'appliquent de la même manière.

Pour préparer la migration d'un XWEB EVO vers un XWEB PRO, contactez Dixell France.

3. Renforcer les comptes et les mots de passe

Les XWEB PRO et EVO sont livrés avec le même compte d'usine : identifiant « Admin », mot de passe « Admin ».
Sur les deux gammes, les comptes se gèrent dans le menu Système → Utilisateurs, selon la même procédure. Les libellés cités ci-après sont ceux de l'interface en français.

Organisation des comptes

- Conservez le mot de passe du compte Admin d'origine sous scellé ou dans un gestionnaire de mots de passe, et ne l'utilisez pas au quotidien.
- Répartissez les profils selon les métiers : consultation pour le personnel du site, paramétrage pour le frigoriste.

Modifier le mot de passe d'un compte (PRO et EVO)

1. Se connecter avec un compte administrateur.
2. Ouvrir le menu Système → Utilisateurs.
3. Sélectionner le compte dans la liste des utilisateurs configurés.
4. Saisir le nouveau mot de passe dans le champ Mot de passe. Sur le XWEB PRO, le saisir une seconde fois dans Confirmer mot de passe et vérifier que la barre de robustesse est verte.
5. Cliquer sur Enregistrer.

Créer un compte nominatif (PRO et EVO)

1. Dans Système → Utilisateurs, cliquer sur + Add, puis choisir Utilisateurs.
2. Renseigner Nom d'utilisateur (identifiant de connexion), Étiquette (nom de la personne) et Mot de passe.
3. Associer le compte à un profil existant : le profil détermine les droits accordés.
4. Pour un prestataire extérieur, renseigner Date d'expiration : passé cette date, le compte est automatiquement désactivé.
5. Cliquer sur Enregistrer.

Activer la politique de mots de passe (PRO uniquement)

Dans Système → Utilisateurs, le bouton Politique de mot de passe donne accès aux règles de sécurité. Celles-ci s'appliquent aux comptes pour lesquels la case Enforce Password Policy est cochée ; nous recommandons de la cocher sur tous les comptes. Lors de l'enregistrement, le XWEB vérifie le mot de passe saisi et affiche un avertissement s'il ne respecte pas ces règles. Suivez les recommandations de complexité comme décrit dans l'avis de sécurité Copeland.

Le XWEB EVO ne propose pas de politique de mots de passe paramétrable. Il bloque toutefois un compte pendant 5 minutes après 5 saisies erronées en 5 minutes.

4. Sécuriser l'accès à distance

Le bulletin de Copeland impose que tout accès à distance passe par un tunnel VPN chiffré, sans redirection de port ni DMZ.

En France, Dixell France suggère trois solutions permettant d'y répondre :

- Un routeur 4G proposé par Dixell France, équipé d'un VPN et d'une carte SIM sans abonnement. Le XWEB est ainsi accessible à distance tout en restant totalement indépendant du réseau du client.

- Le serveur VPN intégré à la box Internet du client. À ce jour, en France, nous constatons que les box Free, Free Pro et Orange Pro proposent nativement cette fonctionnalité sans surcoût. Vérifiez-le auprès de votre opérateur télécom. Il est recommandé de dédier la box au XWEB, afin de ne pas exposer d'autres équipements à cet accès distant.

- Un serveur VPN dédié, mis à disposition par le responsable du réseau informatique du client (par exemple Teltonika, Stormshield ou UniFi).

Par ailleurs, aucun logiciel de prise en main à distance (AnyDesk, TeamViewer ou équivalent) ne doit être installé sur un poste du site laissé allumé en permanence.

Dixell France se tient à votre disposition pour répondre à vos questions.