Ürün Bülteni

XWEB izleme sistemleri için güvenlik bilgilendirmesi

Sayın Müşterimiz, Copeland Controls, 30 yılı aşkın süredir soğutma ve HVAC sektöründe güvenilir bir lider olarak sektör standartlarını belirleyen, güvenilir ve yüksek kaliteli ürünler sunmaktadır. Geçmişimiz; titiz testlere ve güvenilirlik ile performansa yönelik tavizsiz bağlılığa dayanan mükemmeliyet anlayışı üzerine kuruludur. Copeland Controls XWEB izleme üniteleri, yirmi yılı aşkın süredir kritik sektörlerdeki müşterilere güvenilir hizmet vermektedir. Bu süre içinde teknoloji ve güvenlik gereksinimleri önemli ölçüde gelişmiştir; ürünlerimizin günümüz standartlarını karşılamasını sağlamaya kararlıyız. Ürünlerimizin emniyetini, kalitesini ve güvenliğini korumak, yaptığımız her işin ayrılmaz bir parçasıdır. Küresel siber güvenlik topluluğuyla aktif iş birliği yapıyor, bağımsız uzmanları olası güvenlik açıklarını belirlenmiş süreçlerimiz aracılığıyla bildirmeye teşvik ediyoruz. Bu yaklaşım şeffaflığı, güveni ve sürekli iyileştirmeyi desteklemektedir.

Kullanım ömrü sona ermiş ve üretimden kaldırılmış XWEB EVO platformunu ve güncel olmayan yazılım sürümlerini çalıştıran XWEB PRO sistemlerini etkileyen bir siber güvenlik açığına ilişkin bildirimlerden haberdarız. Sorunu tespit ettik ve müşterilerimizin sistemlerini güvence altına almalarına yardımcı olmak amacıyla aşağıdaki önerileri sunuyoruz.

XWEB denetim sistemlerinin güvenli kullanımına yönelik öneriler

Özet

Tüm XWEB sistemlerinin genel internete erişimini derhal kaldırın; ardından yerel ağ üzerinden şüpheli etkinlikleri inceleyin ve gerekirse cihazları geri yükleyin.

Bu bilgilendirme, XWEB denetim sistemleriyle ilişkili siber güvenlik riskini azaltmak için uygulanabilecek ek önlemleri sıralamakta ve izinsiz erişilmiş olabilecek bir ünitenin nasıl kurtarılacağını açıklamaktadır.

1. Geçişinizi planlayın. XWEB EVO hizmet ömrünün sonuna ulaşmıştır ve artık güvenlik yamaları almamaktadır; desteklenen platform XWEB PRO'dur. PRO kullanılsa bile sistemi internete doğrudan açmayın.
2. İnternet erişimini kaldırın. XWEB'e yerel ağınızın dışından erişilemediğinden emin olun (bkz. Acil risk azaltma önlemleri).
3. Üniteyi kontrol edin ve geri yükleyin. Yalnızca yerel ağdan çalışarak adım adım prosedürü izleyin.

Acil risk azaltma önlemleri

İzinsiz erişimden şüphelenip şüphelenmediğinize bakılmaksızın bu önlemleri tüm XWEB sistemlerine uygulayın.

- XWEB'i genel internete kapatın. Port yönlendirme, DMZ veya doğrudan genel IP adresi kullanmayın.
- Fiziksel erişimi yalnızca yetkili personelle sınırlandırın (örneğin ekipman odalarına girebilecek kişileri kısıtlayın ve mümkünse anahtarlı giriş kullanın).
- Uzaktan erişim için VPN hizmeti kullanın; böylece XWEB'e yalnızca kısıtlanmış ve şifreli bir tünel üzerinden erişilsin.

Copeland Controls önerileri

Cihaz kılavuzunda yer alan tüm talimatlara ve teknik özelliklere uyun; aşağıdakiler dahil ancak bunlarla sınırlı olmamak üzere güvenlik alanındaki en iyi uygulamaları hayata geçirin:

- Kontrol sistemini hiçbir zaman genel internete açmayın.
- Güvenlik duvarınızı SSH gibi yönetim protokollerine erişimi kısıtlayacak şekilde yapılandırın.
- Ağınızı, kontrol sistemine gelen ve sistemden giden iletişimi sınırlandıracak şekilde yapılandırın.
- Varsayılan hesap parolalarını değiştirin ve parolaların sektördeki en iyi uygulamalara uygun olmasını sağlayın.
- Denetleyicinin web arayüzünü genel internete açmadan, web tabanlı trafik için HTTPS'yi yapılandırıp etkinleştirin.

Güvenliği ihlal edilmiş olabilecek bir XWEB nasıl kontrol edilir ve geri yüklenir?

XWEB'e yalnızca yerel ağ üzerinden bağlanın ve aşağıdaki adımları sırasıyla uygulayın.

Başlamadan önce

- Üniteyi izole edin. Başlamadan önce XWEB'e yönlendiren tüm port yönlendirme veya DMZ kurallarını kaldırın ya da yönlendiricinin WAN bağlantısını kesin.
- Bulgularınızı kaydedin. Herhangi bir değişiklik yapmadan önce kullanıcı listesi, profiller ve sistem ayarlarının ekran görüntülerini alın. Copeland desteği ve olası bir olay raporu için bunlar gerekebilir.

Prosedür

1. Yönetici parolanızla oturum açın. Parola değiştirilmişse ve oturum açamıyorsanız 7/24 hizmet veren Copeland Teknik Destek ile ColdChain.TechnicalServices@copeland.com adresinden iletişime geçerek geçici erişim parolası almak için talimat isteyin. Destek ekibinin güncel XWEB tarihine ve XWEB oturum açma sayfasında gösterilen MAC adresine ihtiyacı olacaktır. MAC adresini görüntülemek için oturum açma sayfasında CTRL+ALT tuşlarına basın.
2. En son yedeğinizi geri yükleyin. Oturum açtıktan sonra en güncel yedeği geri yüklerken şu seçenekleri seçin: System (Sistem); Devices, Layout, Tools, Users (Cihazlar, Düzen, Araçlar, Kullanıcılar). Yedeğin, şüphelenilen izinsiz erişimden önce oluşturulduğundan emin olun.
3. Yedeğiniz yoksa kullanıcıları ve profilleri kontrol edin. Kullanıcı listesinin beklediğiniz gibi olduğunu doğrulayın; tanımadığınız kullanıcı veya profilleri kaldırın.
4. Tüm kullanıcı parolalarını değiştirin. Her parola şu asgari gereksinimleri karşılamalıdır: en az 8 karakter; en az bir rakam; en az bir büyük harf; en az bir küçük harf; kullanıcı adını içermemeli; ana bilgisayar adını veya sistem adını içermemeli; tek bir karakterin tekrarından oluşmamalıdır (örn. aaaaaaaa). Öneri: 12 veya daha fazla karakter, en az bir özel simge ve her hesap için farklı parola.
5. Yazılımı güncelleyin. Tüm XWEB PRO müşterilerinin mevcut en güncel sürüm olan v1.16.1 sürümüne yükseltme yapması kuvvetle önerilir. XWEB EVO artık desteklenmemektedir; tüm müşterilerin desteklenen bir platforma geçmesi kuvvetle önerilir. XWEB modelinize uygun en son yazılımı Copeland Sistem Yazılımı Güncelleme sayfasından indirip SYSTEM > Update > Updates yolundan yükleyin.
6. Sistem yapılandırmasını gözden geçirin. Ağ ayarları (ağ geçidi ve DNS) ve posta sunucusu ayarları dahil kullanılan tüm hizmetlerin doğru yapılandırıldığını kontrol edin.
7. Alarm yönetimini kontrol edin. Alarm kategorilerinin mevcut ve cihazların alarm değişkenlerine atanmış olduğunu doğrulayın. Gerektiğinde alarm kategorilerinin e-posta veya SMS bildirimi gönderen ya da alarm rölelerini tetikleyen bir seviyeye bağlandığından emin olun. E-posta ve SMS alıcılarının mevcut ve doğru olduğunu kontrol edin. Bildirimlerin gerçekten ulaştığını doğrulamak için test alarmı oluşturun.
8. Varsa yedek dosyalardan cihaz parametrelerini geri yükleyin: (1) DEVICES bölümünden cihazı seçin. (2) Parameters sekmesini açın. (3) Import seçeneğine tıklayıp yedek dosyasını seçin. (4) Parametre değerleri yüklendikten sonra Write seçeneğine tıklayın.
9. Parametre yedekleriniz yoksa her cihazı sırayla seçin, parametrelerini Read komutuyla okuyun ve uygulamaya uygun olduklarını doğrulayın (ayar noktaları, alarm eşikleri, defrost ayarları).
10. Yeni bir yedek oluşturun. Kontroller ve gerekli geri yüklemeler tamamlandığında mutlaka yeni bir yedek oluşturun ve bir kopyasını cihazın dışında saklayın.

Erişimi güvence altına almak için ek öneriler

Bu önlemler, yukarıdaki temel uygulamaların ötesinde en yaygın giriş noktalarını kapatır.

Uzaktan erişim

- VPN hizmetinden yararlanın. Kuruluşunuzun onayladığı VPN hizmetinin uygulanması için BT departmanınıza danışın.

Ağ

- XWEB'i ofis, satış noktası (POS) ve misafir Wi-Fi ağlarından ayrı, kendisine ayrılmış bir ağ bölümüne (VLAN) yerleştirin.
- Yalnızca XWEB'in ihtiyaç duyduğu dışa giden trafiğe (örneğin posta sunucusu, DNS, NTP ve Copeland güncelleme sunucusu) izin verin; diğer tüm trafiği engelleyin.
- Dışarıdan erişilebilirliği doğrulayın: Tesis ağı dışındaki bir bağlantıdan, örneğin Wi-Fi kapatılmış bir telefondan, tesisin genel IP adresini tarayıcıda açmayı deneyin. XWEB oturum açma sayfası görünmemelidir.

Hesaplar ve parolalar

- Her kullanıcının kendisine ait, adı belirli ve benzersiz bir hesabı olmalıdır; ortak hesaplara izin verilmemelidir.
- Her hesaba görev için uygun en kısıtlayıcı profili atayın ve yönetici yetkilerini bir veya iki kişiyle sınırlandırın.
- Artık gerekmeyen hesapları devre dışı bırakın veya silin; kullanıcı listesini yılda en az bir kez gözden geçirin.
- Ayrıcalıklı bir hesabın kullanıldığı her harici servis ziyaretinden sonra parolaları değiştirin.
- XWEB parolalarını başka yerlerde asla yeniden kullanmayın; parolaları tesis, mağaza veya kurulum firmasının adına dayandırmayın.

İzleme ve yedeklemeler

- Sistem yapılandırmasını ve cihaz parametrelerini düzenli bir takvime göre ve her önemli değişiklikten sonra yedekleyin; kopyaları cihazın dışında saklayın.
- Kayıtların ve günlüklerin doğru zaman damgaları taşıması için XWEB saatini NTP ile senkronize tutun.

İzinsiz erişimden şüpheleniyorsanız

- Önce üniteyi izole edin, ardından kurtarma işlemini gerçekleştirin (bkz. Başlamadan önce).
- Ürün sıcaklıklarını doğrudan soğutmalı teşhir dolaplarından kontrol edin: değiştirilmiş ayar noktaları veya alarm eşikleri gıda güvenliğini riske atabilir.
- Copeland Teknik Destek ekibine, BT veya güvenlik ekibinize ve gerektiğinde yetkili makama (ABD'de CISA) bildirimde bulunun.

XWEB PRO'ya geçişinizi planlayın

XWEB EVO hizmet ömrünün sonuna ulaşmıştır ve artık yazılım güncellemesi veya güvenlik yaması almayacaktır. Aktif olarak bakımı yapılan ve düzenli olarak güncellenen mevcut platform XWEB PRO'ya geçmenizi kuvvetle öneriyoruz.

Teknik destek

Copeland Teknik Destek ekibine teknik.destek@ercanteknik.com, dixell.service@copeland.com, ColdChain.TechnicalServices@copeland.com adreslerinden ulaşabilirsiniz.