SONY

Yardım Kılavuzu

MPC-2610

Güvenlik Önlemleri

Bu Yardım Kılavuzu, ünite kullanılarak dosya aktarımı ve yayın yapılması için güvenlik önlemlerini açıklamaktadır.

MPC-2610
Güvenlik Önlemleri

Güvenlik Önlemleri

Bu konu başlığında, ünite bir ağa bağlanacağında alınacak önlemler açıklanmaktadır.

- İletişim içeriği, sinyallerin yakınında bulunan izinsiz üçüncü şahıslar tarafından kasıtsız olarak kesilebilir. Kablosuz LAN iletişimi kullanırken iletişim içeriğini korumak için gerekli güvenlik önlemlerini doğru şekilde uygulayın.
- [Security] kablosuz LAN ayarını [None] olarak ayarlayıp bir erişim noktasına bağlandığınız takdirde, kamera ile erişim noktası arasındaki kablosuz iletişim şifrelenmez ve sinyal aralığında olan bir üçüncü taraf tarafından kesilebilir. Gelişmiş güvenlik için WPA2 veya WPA3 güvenlik protokolünü kullanın.
- SONY; İLETİM ARAÇLARI ÜZERİNDEKİ GÜVENLİK ÖNLEMLERİNE UYGUN YAPILMAYAN UYGULAMA HATASINDAN KAYNAKLI HERHANGİ BİR ZARARDAN, İLETİM ÖZELLİKLERİNDEN YA DA HERHANGİ BİR GÜVENLİK SORUNUNDAN KAYNAKLI ÖNLENEMEZ VERİ SIZINTILARINDAN SORUMLU OLMAYACAKTIR.
- Çalışma ortamına bağlı olarak ağ üzerindeki izinsiz üçüncü kişiler cihaza erişebilir. Cihazı ağa bağlarken mutlaka ağın güvenli şekilde korunduğunu onaylayın.
- Bu ürünü bir ağa bağlarken, yönlendirici veya güvenlik duvarı gibi koruma işlevi sağlayan bir sistem üzerinden bağlayın. Bu tür bir koruma olmadan bağlanırsa, güvenlik sorunları oluşabilir.

TP1002221057

MPC-2610
Güvenlik Önlemleri

İnternet Bağlantısı Önlemleri

Bu konu başlığında, ünite internete bağlanacağında alınacak önlemler açıklanmaktadır.

- Ünite, kablosuz LAN ile yalnızca açıkları bulunan güvenlik yöntemleri olan WEP veya WPA'yı kullanan erişim noktalarına bağlanamaz.
- Ünite bir ağ cihazı (örneğin; bir yönlendirici veya anahtarlama hub'ı) değildir. Üniteyi ağ ayarlarını DoS (Hizmet Reddi) saldırıları gibi ağ tabanlı saldırılara karşı uygun şekilde korumak için yapılandırabileceğiniz ve yönetebileceğiniz bir ağa bağlamanız önemle önerilir.
- Üniteyi bir ağa bağlarken uygun şekilde yapılandırılmış ve yönetilen bir yönlendirici üzerinden bağlayın veya aynı işlevlere sahip bir LAN bağlantı noktasına bağlayın. Böyle bir koruma olmadan bağlantı sağlandığı takdirde (örneğin ücretsiz Wi-Fi hatları kullanılarak bağlantı yapıldığında) güvenlik sorunları oluşabilir. Uygun şekilde yapılandırıldığında, yönlendiriciler DoS saldırılarına ya da ağdaki cihazların işlev kaybına karşı yeterli korumayı sağlar. Olağan dışı bir durum fark ederseniz, derhal kameranın ağ ile bağlantısını kesin.

TP1002221058

MPC-2610
Güvenlik Önlemleri

Ağ İşlevi ile İlgili Önlemler

Bu konu başlığında, ünitenin ağ işlevi ile ilgili önlemler açıklanmaktadır.

- Yetkisiz erişim tespit edildiği takdirde, kamera iletişimleri kabul etmeyebilir. Bu durum oluşursa, en baştan yeniden bağlantı kurun.
- [Network] – [Network Setup] – [Show Authentication] kullandığınızda üniteyi bağlamak için kimlik bilgileri görüntülenir. Başkalarının ekranı görmemesine ve QR kodu görüntüsünü kopyalamamasına dikkat edin.
- Satın alım sırasında bir kullanıcı adı ve parola belirlenmelidir. Kullanıcı adınızı ve parolanızı ayarlarken, bu ayarları başkalarının görmemesi için dikkatli olun. Kullanıcı adınızı ve şifrenizi aşağıdaki gibi ayarlayın.

[User Name]	– 1 ile 16 karakterden oluşan bir kullanıcı adı belirleyin. – Bu, fabrika varsayılan ayarı olarak “admin” olarak ayarlanmıştır. – Geçerli semboller şunlardır. Alfabetik karakterler (büyük ve küçük harf), sayısal karakterler, semboller (! % + , - . = _)
[Password]	– En az 1 veya daha fazla alfabetik karakter ve 1 veya daha fazla sayısal karakter içeren 8 ila 16 karakterden oluşan bir şifre belirleyin. – Geçerli semboller şunlardır. Alfabetik karakterler (büyük ve küçük harf), sayısal karakterler, semboller (! % + , - . = _)

TP1002221059

MPC-2610
Güvenlik Önlemleri

Kablosuz LAN ile İlgili Önlemler

Bu konu başlığında, ünite kablosuz LAN ile bağlanacağında alınacak önlemler açıklanmaktadır.

- Bu ünitenin Yardım Kılavuzunda, kablosuz LAN erişim noktaları ve LAN bağlantılarını aktaran kablosuz LAN yönlendiricileri “erişim noktası” olarak ifade edilmektedir.
- [Security] (şifreleme yöntemi) [None], [WPA2] veya [WPA3] olarak ayarlanabilir. Güvenlik açısından [WPA2] veya [WPA3] kullanılması önerilir. [None] seçildiğinde bağlanmadan önce bir mesaj görüntülenir. Güvenli bir kablosuz LAN bağlantısı için, WPA2 veya WPA3 güvenlik ayarı olan erişim noktalarına bağlanılması önemle önerilir.
- [Manual Register] kullanılarak bir kablosuz LAN erişim noktası kaydedilirken varsayılan olarak WPA2 güvenlik yöntemi seçilir.
- Bir erişim noktasına herhangi bir güvenlik ayarı olmadan bağlanmanız halinde, korsanlık girişimlerine, kötü amaçlı üçüncü tarafların erişimine veya güvenlik açıklarına yönelik saldırılara maruz kalabilirsiniz. Aksinin kaçınılmaz olduğu durumlar haricinde, herhangi bir güvenlik ayarı olmadan bağlantı yapılması önerilmez.
- Bir kablosuz LAN'da güvenliğin yapılandırılması büyük önem taşır. Sony, güvenlik önlemlerinin alınmamasından ya da kablosuz LAN kullanım koşulundaki kaçınılamayacak durumlardan dolayı bir güvenlik sorununun oluşmasından sorumlu tutulamaz.

TP1002221060

MPC-2610
Güvenlik Önlemleri

USB Bağlantısı ile ilgili Önlemler

Bu konu başlığında, ünite USB ile bağlanacağında alınacak önlemler açıklanmaktadır.

- Bağlantı için yalnızca güvenilen akıllı telefonlar kullanın. Güvenlik ile ilgili endişeler nedeniyle kaynağı bilinmeyen cihazların bağlanması önerilmez.

TP1002221061

FTPES (FTPS) İşlevi Hakkında

FTPS işlevi, güvenli dosya aktarımını sağlamak için çeşitli şifreleme algoritmalarını destekler. Birçok çeşitli sunucu ile uyumluluğun sağlanması için bazıları geçerli güvenlik en iyi uygulamaları ile uyumlu olmayabilecek birden fazla şifreleme algoritması desteklenir.

FTPS işlevi tarafından desteklenen şifreleme algoritmaları

Aşağıdaki şifreleme algoritmaları desteklenir.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Önerilen şifreleme algoritmaları

NIST önerileri (NIST SP 800-57 Bölüm 1 Revizyon 5) ve ilgili güvenlik standartlarına dayalı olarak aşağıdaki şifreleme algoritmaları önerilir.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Artık kullanılmayan algoritmalar hakkında

FTPS işlevi uyumluluk için aşağıdaki algoritmaları da destekler ancak bunlar NIST önerileri (NIST SP 800-57 Bölüm 1 Revizyon 5) ve ilgili güvenlik standartları nedeniyle artık kullanılmamaktadır ve ilerideki sürümlerde kullanımdan kaldırılabilir.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Bağlantı uyumluluğu için

FTPS işlevi, güvenlik ve uyumluluk arasında bir denge kurularak geliştirilmiştir. Mevcut durumda, artık kullanılmayan algoritmalar aşağıdaki nedenlerle desteklenmektedir ancak ileride güvenliği iyileştirmek için bunların kaldırılması mümkündür.

- Serbest çalışan fotoğrafçı ve videografikerlerin çeşitli istemcilerde çalışan sunuculara bağlanması gerekir.
- Daha eski sistemler ve eski sunucular ile uyumluluğun korunması gerekir.
- Sunucu tarafında şifreleme algoritması ayarlarının değiştirilmesi karmaşık bir süreç olduğundan tüm kullanıcılar daha güvenli bir ortama geçmek için gerekli hazırlıkları yapmamış olabilir.
- FTPS ayarları sıklıkla diğer güvenli hizmetler ile paylaşılır. Sunucu üzerindeki diğer hizmetler üzerinde bir etki yaratabileceklerinden her türlü değişikliğin dikkatlice düşünülmesi gerekir.
- Farklı ortamlarda çalışabilirlik için geniş bir şifreleme algoritması aralığının desteklenmesi şarttır.

Bir FTPS bağlantısı sırasında kullanılan şifreleme algoritması, hedef sunucu ile otomatik anlaşma yoluyla belirlendiğinden, sunucu ayarlarına bağlıdır. Mevcut durumda kullanıcıların çeşitli ihtiyaçlarını karşılamak üzere güvenlik risklerinin bilincinde olunarak uyumluluğa öncelik verilmektedir.

Güvenlik riskleri

CBC/DHE/RSA/SHA-1'i de içeren eski algoritmaların kullanılması, saldırgan tarafından şifrelenmiş verilerin şifresinin çözülmesi ya da bu verilere müdahale edilmesi, bunun sonucunda da aktarım sırasında verilerin açığa çıkması riskini artırır.

Güvenli bağlantı için öneri

FTPS işlevini kullanmadan önce bağlantı hedef sunucusunun önerilen şifreleme algoritmasını destekleyip desteklemediğini kontrol edin. Sunucu tarafında yalnızca önerilen algoritmaları etkinleştirin ve artık kullanılmayan algoritmaları devre dışı bırakın.

Güvenli FTP kullanarak karşıya yükleme

Hedef dosya sunucusuna bağlantı için FTPS (FTPES) kullanarak dosyaları şifrelenmiş olarak yükleyebilirsiniz.
Güvenli FTP aktarımı için dosya aktarımı hedef sunucu ayarlarında [Using Secure Protocol] ayarını [On] olarak ayarlayın ve bir sertifika içe aktarın.

Referanslar

- Recommendation for Key Management, Special Publication 800-57 Part 1 Revision 5, NIST, 2020.
- Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication 800-131A Revision 2, NIST, 2019.
- Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, NIST, 2005 (10/06/2016 itibarıyla yapılan güncellemeler ile birlikte).

Sertifika

FTPES (FTPS) işlevi tarafından kullanılan sertifikayı bir hafıza kartının kök dizinine yazın. Dosya adını aşağıdaki gibi ayarlayın.
certification.pem (PEM biçimi)
Karşıya yüklenebilecek maksimum sertifika boyutu, her bir sertifika için 1 MB'dir.

TP1002221062