MPC-2610

Предпазни мерки за сигурност

Този Помощен наръчник описва предпазните мерки за сигурност при прехвърляне на файлове и стрийминг чрез уреда.

Предпазни мерки за сигурност

Предпазни мерки при връзка с интернет

Предпазни мерки, свързани с мрежовата функция

Предпазни мерки, свързани с безжичната локална мрежа (LAN)

Предпазни мерки, свързани с USB тетъринг

Относно функцията FTPES (FTPS)

MPC-2610
Предпазни мерки за сигурност

Предпазни мерки за сигурност

Тази тема описва предпазните мерки при свързване на уреда към мрежа.

- Съдържанието на комуникацията може да бъде неусетно прихванато от неоторизирани трети страни в обсега на сигналите. Когато използвате безжична LAN комуникация прилагайте внимателно мерките за сигурност, за да защитите съдържанието ѝ.
- Ако при настройка на [Security] на безжичната LAN мрежа изберете [None] и свържете с точка за достъп, безжичната комуникация между камерата и точката на достъп няма да бъде криптирана и е възможно да бъде прихванатата от трета страна в обсега на сигнала. Използвайте протокол за защита WPA2 или WPA3 за повишена защита.
- SONY НЕ НОСИ ОТГОВОРНОСТ ЗА ЩЕТИ ОТ КАКЪВТО И ДА Е ВИД, ПРОИЗТИЧАЩИ ОТ НЕСПАЗВАНЕТО НА ПРАВИЛНИ МЕРКИ ЗА СИГУРНОСТ НА ПРЕДАВАТЕЛНИТЕ УСТРОЙСТВА, НЕИЗБЕЖНОТО ИЗТИЧАНЕ НА ДАННИ, В РЕЗУЛТАТ ОТ СПЕЦИФИКАЦИИТЕ ЗА ПРЕДАВАНЕ, ИЛИ КАКВИТО И ДА БИЛО ПРОБЛЕМИ СЪС СИГУРНОСТТА.
- В зависимост от работната среда до уреда може да имат достъп неупълномощени трети лица в мрежата. При свързване на уреда към мрежата се постарайте да се уверите, че мрежата е защитена сигурно.
- Когато свързвате този продукт към мрежа, свържете го чрез система, която предоставя защитна функция, напр. рутер или защитна стена. Ако е свързан без такава защита, може да възникнат проблеми, свързани със сигурността.

TP1002220927

MPC-2610
Предпазни мерки за сигурност

Предпазни мерки при връзка с интернет

Тази тема описва предпазните мерки при свързване на уреда към интернет.

- Уредът не може да се свързва чрез безжична LAN мрежа с точка за достъп, която използва единствено WEP или WPA, методи с уязвимости.
- Уредът не е мрежово устройство (например рутер или мрежов комуникатор). Силно се препоръчва да свържете устройството към мрежа, където можете да конфигурирате и управлявате мрежовите настройки по подходящ начин, за да се предпазите от мрежови атаки, като например DoS атаки (атаки за отказ на услуга).
- Когато свързвате уреда към мрежа, свържете го чрез рутер, който е настроен и управляван по подходящ начин или го свържете към LAN порт, който извършва същите функции. Ако бъде свързан без подобна защита (например чрез Wi-Fi мрежа със свободен достъп), може да настъпят проблеми със сигурността. Когато са правилно конфигурирани, рутерите предоставят достатъчна защита срещу DoS атаки или загуба на функционалност на устройства в мрежата. Ако забележите нещо необичайно, незабавно прекратете връзката на камерата с мрежата.

TP1002220928

MPC-2610
Предпазни мерки за сигурност

Предпазни мерки, свързани с мрежовата функция

Тази тема описва предпазните мерки относно мрежовата функция на уреда.

- Ако бъде засечен неоторизиран достъп, камерата може да спре да приема комуникации. Ако това се случи, свържете се отново отначало.
- Информацията за удостоверяване за свързване на уреда се показва, когато използвате [Network] – [Network Setup] – [Show Authentication]. Уверете се, че екранът не се вижда и изображението с QR код не може да бъде копирано от някой друг.
- Потребителското име и паролата трябва да бъдат настроени в момента на покупка. Когато настройвате потребителското име и паролата си, се уверете, че настройките не са видими за някой друг. Задайте потребителското име и паролата както следва.

[User Name]	– Задайте потребителско име, което съдържа от 1 до 16 знака. – То е настроено фабрично на “admin” по подразбиране. – Следните символи са валидни за въвеждане. Букви (главни и малки), цифри, символи (! % + , - . = _)
[Password]	– Задайте парола, съдържаща от 8 до 16 знака и поне 1 или повече букви и 1 или повече цифри. – Следните символи са валидни за въвеждане. Букви (главни и малки), цифри, символи (! % + , - . = _)

TP1002220929

MPC-2610
Предпазни мерки за сигурност

Предпазни мерки, свързани с безжичната локална мрежа (LAN)

Тази тема описва предпазните мерки при свързване на уреда чрез безжична LAN мрежа.

- В Помощния наръчник за този уред точките за достъп до безжична LAN мрежа и рутерите за безжична LAN мрежа, които препредават LAN връзки, се наричат “точки за достъп”.
- [Security] (метод на криптиране) може да бъде настроен на [None], [WPA2], или [WPA3]. Използването на [WPA2] или [WPA3] се препоръчва от гледна точка на сигурността. Когато е избрано [None], преди свързването се показва съобщение. За сигурна безжична LAN връзка силно се препоръчва свързване към точки за достъп с настройки за сигурност WPA2 или WPA3.
- По подразбиране е избран методът за сигурност WPA2, когато се регистрира точка за достъп до безжична LAN мрежа с използване на [Manual Register].
- Ако се свържете с точка за достъп без настройка за сигурност, може да станете обект на хакерска атака, достъп от злонамерени трети страни или атаки, базирани на уязвимости. Освен ако не е неизбежно, не се препоръчва връзка без каквато и да е настройка за сигурност.
- Настройването на сигурността при безжична LAN мрежа е изключително важно. Sony няма да носи отговорност за щети, получени в резултат от невзети мерки за сигурност, или за проблеми със сигурността, възникнали, поради неизбежни обстоятелства при използването на безжична LAN връзка.

TP1002220930

MPC-2610
Предпазни мерки за сигурност

Предпазни мерки, свързани с USB тетъринг

Тази тема описва предпазните мерки при свързване на уреда чрез USB тетъринг.

- Използвайте единствено доверени смартфони за тетъринг. Свързването с непознати устройства не се препоръчва поради съображения за сигурност.

TP1002220931

Относно функцията FTPES (FTPS)

Функцията FTPS поддържа различни алгоритми за криптиране, за да осигури защитен трансфер на файлове. Множество от алгоритмите за криптиране, някои от които може и да не отговарят на съвременните най-добри практики за сигурност, се поддържат заради съвместимостта им с широк набор от сървъри.

Алгоритмите за криптиране се поддържат от функцията FTPS

Поддържат се следните алгоритми за криптиране:

- 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

Препоръчителни алгоритми за криптиране

Следните алгоритми за криптиране са препоръчителни въз основа на препоръките на Националния институт за стандарти и технологии (NIST) (NIST SP 800-57 част 1, редакция 5) и други свързани стандарти за сигурност:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Относно непрепоръчителните алгоритми

Функцията FTPS поддържа също и следните алгоритми за съвместимост, но те не се препоръчват, въз основа на препоръките на NIST, (NIST SP 800-57 част 1, редакция 5) и други свързани стандарти за сигурност и може да бъдат премахнати в бъдеща версия:

- 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

Относно съвместимостта на връзката

Функцията FTPS е проектирана за баланс между сигурност и съвместимост. Към момента непрепоръчителните алгоритми се поддържат по следните причини, но те може да бъдат премахнати в бъдещи версии с цел подобряване на сигурността:

- Фотографи и видеооператори на свободна практика се нуждаят от връзка със сървъри на различни клиенти.
- Съвместимостта със стари системи и остарели сървъри трябва да се поддържа.
- Не всички потребители са готови да преминат към по-безопасни настройки, тъй като промяната в настройките на алгоритъма за криптиране на сървъра е сложна.
- Настройките на FTPS често се споделят с други защитени услуги. Всякакви промени трябва да бъдат обмислени внимателно, тъй като те може да окажат въздействие върху други услуги на сървъра.
- Трябва да се поддържа голям набор от алгоритми за криптиране, за да се осигури оперативна съвместимост в различни среди.

Алгоритъмът за криптиране, използван по време на FTPS връзка се определя чрез автоматично установяване на връзка със сървъра на дестинацията и следователно зависи от настройките на сървъра. Въпреки че рисковете за сигурността са познати, към момента с приоритет е съвместимостта с цел да се задоволят разнообразните нужди на потребителите.

Рискове за сигурността

Употребата на непрепоръчителни алгоритми, включително CBC/DHE/RSA/SHA-1, повишава риска от декриптиране на криптираните данни или намесата от нападател, който да разкрие данни по време на трансфер.

Препоръки за безопасна връзка

Преди употреба на функцията FTPS проверете дали сървърът на дестинация на връзката поддържа препоръчителните алгоритми за криптиране. Активирайте единствено препоръчаните алгоритми от страна на сървъра и деактивирайте непрепоръчителните алгоритми.

Качване чрез защитен FTP

Можете да качвате файлове с криптиране с използване на FTPS в режим Explicit (FTPES) за връзка с файловия сървър на местоназначението.
За сигурен FTP трансфер, настройте [Using Secure Protocol] на [On] в настройките на сървъра на дестинацията за трансфер на файлове и импортирайте сертификат.

Справки

- 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 (съдържа актуализации от 10.06.2016 г.).

Сертификат

Запишете сертификата, използван от функцията FTPES (FTPS), в коренната директория на картата памет.
Променете името на файла на следното:
certification.pem (формат PEM)
Максималната големина на сертификат, който може да бъде зареден, е 1 MB на сертификат.

TP1002220932