ILME-FX6

Запобіжні заходи

У цьому довідковому посібнику описано запобіжні заходи щодо передавання файлів і прямої трансляції за допомогою пристрою.

Запобіжні заходи

У цьому розділі описано запобіжні заходи під час підключення пристрою до мережі.

- Можливе навіть мимовільне перехоплення матеріалів, які передають по каналах зв'язку, неуповноваженими третіми особами, що перебувають поблизу від джерел сигналів. У разі використання для зв'язку бездротових локальних мереж слід вжити відповідні заходи безпеки для забезпечення захисту матеріалів, що передаються по каналах зв'язку.
- Якщо для параметра бездротової локальної мережі [Security] встановити значення [None] і підключитися до точки доступу, бездротовий зв'язок між камерою і точкою доступу не буде зашифровано та може бути перехоплено сторонніми особами в межах радіуса дії сигналу. Для забезпечення посиленого рівня безпеки використовуйте протокол WPA2 або WPA3.
- КОРПОРАЦІЯ SONY НЕ НЕСЕ ЖОДНОЇ ВІДПОВІДАЛЬНОСТІ ЗА БУДЬ-ЯКУ ШКОДУ, ЩО СТАЛА РЕЗУЛЬТАТОМ НЕНАЛЕЖНОГО ВПРОВАДЖЕННЯ ЗАХОДІВ БЕЗПЕКИ НА ПЕРЕДАВАЛЬНИХ ПРИСТРОЯХ, НЕВІДВОРОТНИХ ВИТОКІВ ДАНИХ, СПРИЧИНЕНИХ ТЕХНІЧНИМИ ХАРАКТЕРИСТИКАМИ ПЕРЕДАЧІ ДАНИХ, АБО ПРОБЛЕМ З БЕЗПЕКОЮ БУДЬ-ЯКОГО ТИПУ.
- Наявні у мережі неуповноважені треті особи можуть отримати доступ до пристрою в залежності від умов експлуатації. Перед під'єднанням пристрою до мережі слід переконатися у надійності захисту останньої.
- В разі під'єднання цього виробу до мережі слід під'єднувати його за допомогою системи, що має захисні функції, як-от роутер або брандмауер. В разі під'єднання без використання такої системи можуть виникнути проблеми з безпекою.

TP1002274662

Застереження щодо підключення до Інтернету

У цьому розділі описано запобіжні заходи під час підключення пристрою до Інтернету.

- Цей пристрій не може підключатися через бездротову локальну мережу до точки доступу, яка використовує лише протоколи WEP або WPA — методи захисту, які мають вразливості.
- Цей пристрій не є мережевим пристроєм (наприклад, маршрутизатором або концентратором-комутатором). Наполегливо рекомендовано підключати пристрій до мережі, у якій можна належним чином конфігурувати налаштування мережі та керувати ними, щоб захиститися від мережевих атак, таких як DoS-атаки (атаки типу «відмова в обслуговуванні»).
- Коли підключаєте пристрій до мережі, робіть це через маршрутизатор, який сконфігурований і керується відповідним чином, або підключайте його до порту локальної мережі з такими самими функціями. У разі підключення без такого захисту (наприклад, якщо використовується безкоштовний Wi-Fi) можуть виникнути проблеми з безпекою. Коли маршрутизатори налаштовано належним чином, вони забезпечують достатній захист від DoS-атак або втрати функціональності пристроїв у мережі. Якщо ви помітите щось незвичне, негайно від'єднайте камеру від мережі.

TP1002274663

ILME-FX6
Запобіжні заходи

Застереження стосовно мережевої функції

У цьому розділі описано застереження стосовно мережевої функції пристрою.

- У разі виявлення несанкціонованого доступу камера може втратити можливість приймати дані, що передаються. У такому випадку встановіть з'єднання заново.
- Натисніть кнопку [Show Authentication] на екрані стану системи [Network], щоб відобразити інформацію для автентифікації підключення до пристрою. Потурбуйтеся про те, щоб сторонні особи не могли побачити екран і скопіювати зображення QR-коду.
- На момент покупки ім'я користувача й пароль автоматично згенеровано та встановлено на камері. Коли встановлюєте ім'я користувача й пароль, переконайтеся, що ці налаштування ніхто не бачить. Встановлюйте ім'я користувача та пароль, як зазначено нижче.

[User Name]	– Встановлюйте ім'я користувача, що складається з 1–16 символів. – У заводських налаштуваннях за замовчуванням для цього параметра встановлено значення «admin». – Дозволені для вводу символи перелічено нижче. Літери (верхнього й нижнього регістрів), цифри, спеціальні символи (! % + , - . = _)
[Password]	– Встановлюйте пароль, що складається з 8–16 символів і містить щонайменше 1 літеру та 1 цифру. – Дозволені для вводу символи перелічено нижче. Літери (верхнього й нижнього регістрів), цифри, спеціальні символи (! % + , - . = _)

TP1002274664

Застереження стосовно бездротової локальної мережі

У цьому розділі описано запобіжні заходи під час підключення пристрою за допомогою бездротової локальної мережі.

- У довідковому посібнику до цього пристрою точки доступу до бездротової локальної мережі та маршрутизатори бездротової локальної мережі, які передають з'єднання з локальною мережею, називаються «точками доступу».
- Для параметра [Security] (метод шифрування) можна встановити значення [None], [WPA2] або [WPA3]. З міркувань безпеки рекомендовано використовувати [WPA2] або [WPA3]. Якщо вибрано [None], перед підключенням відображається повідомлення. Для безпечного під'єднання до бездротової локальної мережі наполегливо рекомендовано підключатися до точок доступу з налаштуваннями безпеки WPA2 або WPA3.
- У разі реєстрації точки доступу бездротової локальної мережі за допомогою [Manual Register] за замовчуванням вибирається метод захисту WPA2.
- Якщо ви підключаєтеся до точки доступу без жодних налаштувань безпеки, то можете стати об'єктом зламу, доступу зловмисників або атак на вразливі місця. За винятком випадків, коли цього не можна уникнути, підключатися до точки доступу без налаштувань безпеки не рекомендовано.
- Конфігурування безпеки бездротової локальної мережі є дуже важливим. Компанія Sony не несе відповідальності за жодні збитки, що виникли через те, що не було вжито заходів безпеки, або якщо проблема з безпекою виникла через непереборні обставини під час використання бездротової мережі.

TP1002274665

Застереження стосовно прив'язки USB

У цьому розділі описано запобіжні заходи під час підключення пристрою за допомогою прив'язки USB.

- Для прив'язки використовуйте лише довірені смартфони. Під'єднання до пристроїв невідомого походження не рекомендовано з міркувань безпеки.

TP1002274666

Про функцію FTPES (FTPS)

Функція FTPS підтримує різні алгоритми шифрування для забезпечення захищеного передавання файлів. Кілька алгоритмів шифрування, деякі з яких можуть не відповідати сучасним стандартам безпеки, підтримуються для сумісності із широким колом серверів.

Алгоритми шифрування, що підтримуються функцією FTPS

Підтримуються зазначені нижче алгоритми шифрування.

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 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

Рекомендовані алгоритми шифрування

Зазначені нижче алгоритми шифрування рекомендовано на основі рекомендацій NIST (NIST SP 800-57, частина 1, редакція 5) і відповідних стандартів безпеки.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Про застарілі алгоритми

Функція FTPS також підтримує зазначені нижче алгоритми для забезпечення сумісності, але вони вважаються застарілими відповідно до рекомендацій NIST (NIST SP 800-57, частина 1, редакція 5) та відповідних стандартів безпеки і їх може бути вилучено в одній з наступних версій.

- 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

Про сумісність підключень

Функцію FTPS розроблено з урахуванням балансу між безпекою та сумісністю. Наразі застарілі алгоритми підтримуються з перелічених нижче причин, але їх може бути вилучено в одній з наступних версій для підвищення рівня безпеки.

- Фотографам і відеооператорам, які працюють як фрілансери, потрібно підключатися до серверів, що працюють на різних клієнтах.
- Потрібно підтримувати сумісність зі старішими системами й попередніми серверами.
- Не всі користувачі готові перейти на безпечніші налаштування, оскільки зміна налаштувань алгоритму шифрування на стороні сервера є складним завданням.
- Налаштування FTPS часто є спільними з іншими захищеними сервісами. Будь-які зміни мають бути ретельно обмірковані, оскільки вони можуть вплинути на інші сервіси на сервері.
- Для забезпечення функціональної сумісності в різних середовищах необхідно підтримувати широке коло алгоритмів шифрування.

Алгоритм шифрування, який використовується під час FTPS-з'єднання, визначається шляхом автоматичного узгодження із сервером призначення, а отже залежить від налаштувань сервера. Незважаючи на наявність ризиків для безпеки, сумісність наразі є пріоритетом для задоволення різноманітних потреб користувачів.

Ризики для безпеки

Використання застарілих алгоритмів, зокрема CBC/DHE/RSA/SHA-1, підвищує ризик розшифровування зашифрованих даних зловмисником і внесення в них несанкціонованих змін, внаслідок чого дані можуть бути незахищеними під час передавання.

Рекомендації щодо безпечного з'єднання

Перед використанням функції FTPS перевірте, чи підтримує сервер адресата з'єднання рекомендований алгоритм шифрування. Увімкніть лише рекомендовані алгоритми на стороні сервера й вимкніть застарілі алгоритми.

Вивантаження з використанням захищеного передавання FTP

Існує можливість вивантаження файлів з шифруванням з використанням протоколу FTPS in Explicit mode (FTPES) для з'єднання з сервером-адресатом.
Для захищеного передавання FTP встановіть для параметра [Using Secure Protocol] значення [On] у налаштуваннях цільового сервера передавання файлів та імпортуйте сертифікат.

Посилання

- 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 (включає оновлення станом на 06.10.2016).

Сертифікат

Запишіть сертифікат, використовуваний функцією FTPES (FTPS), у кореневий каталог карти пам'яті. Задайте назву файлу, як зазначено нижче.
certification.pem (формат PEM)
Максимальний розмір сертифіката, який можна завантажити, становить 1 МБ на один сертифікат.

TP1002274667