MPC-2610

Предупреждения по мерам безопасности

В данном Справочном руководстве приведены предупреждения по мерам безопасности при передаче файлов и потоковой передаче с помощью устройства.

MPC-2610
Предупреждения по мерам безопасности

Предупреждения по мерам безопасности

В этом разделе рассматриваются меры предосторожности при подключении устройства к сети.

- Передаваемое содержимое может быть непреднамеренно перехвачено третьими лицами, находящимися в зоне действия сигнала. Используя беспроводную локальную сеть, принимайте необходимые меры для обеспечения безопасности передачи содержимого.
- Если задать для настройки [Security] беспроводной ЛВС значение [None] и подключить камеру к точке доступа, беспроводная связь между камерой и точкой доступа не будет шифроваться и возможен перехват третьими лицами, находящимися в зоне приема сигнала. Для усиления безопасности используйте протокол безопасности WPA2 или WPA3.
- КОМПАНИЯ SONY НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА КАКОЙ БЫ ТО НИ БЫЛО УЩЕРБ, ВОЗНИКШИЙ ВСЛЕДСТВИЕ НЕСОБЛЮДЕНИЯ МЕР ПРЕДОСТОРОЖНОСТИ ПРИ ИСПОЛЬЗОВАНИИ УСТРОЙСТВ ПЕРЕДАЧИ ДАННЫХ, НЕИЗБЕЖНЫХ УТЕЧЕК ИНФОРМАЦИИ, СВЯЗАННЫХ СО СПЕЦИФИКАЦИЯМИ ПЕРЕДАЧИ ДАННЫХ, ИЛИ ПРОБЛЕМ БЕЗОПАСНОСТИ ЛЮБОГО РОДА.
- В зависимости от операционной среды возможен несанкционированный доступ посторонних лиц к устройству. При подключении устройства к сети убедитесь в том, что сеть надежно защищена.
- При подключении этого изделия к сети выполняйте подключение через систему, которая обеспечивает функцию защиты, такую как маршрутизатор или брандмауэр. При подключении без такой защиты могут возникнуть проблемы с безопасностью.

TP1002221105

MPC-2610
Предупреждения по мерам безопасности

Меры предосторожности при подключении к Интернету

В этом разделе рассматриваются меры предосторожности при подключении устройства к Интернету.

- Данное устройство не может подключаться по беспроводной ЛВС к точке доступа, использующей только протокол WEP или WPA, которые представляют собой методы обеспечения безопасности, имеющие уязвимости.
- Данное устройство не является сетевым устройством (таким как маршрутизатор или концентратор-коммутатор). Настоятельно рекомендуется подключать устройство к сети, в которой можно задавать сетевые настройки и управлять ими так, чтобы обеспечить защиту от сетевых атак, таких как DoS-атаки (атаки типа “отказ в обслуживании”).
- Подключайте устройство к сети через настраиваемый и управляемый соответствующим образом маршрутизатор либо подключайте его к порту ЛВС с такой же функциональностью. При подключении без такой защиты (например, при использовании бесплатного Wi-Fi) могут возникнуть проблемы с безопасностью. Настроенные должным образом маршрутизаторы обеспечивают достаточную защиту от DoS-атак или потери работоспособности устройств в сети. Заметив что-либо необычное, немедленно отключите камеру от сети.

TP1002221106

Меры предосторожности в отношении сетевой функции

В этом разделе рассматриваются меры предосторожности относительно сетевой функции устройства.

- В случае обнаружения несанкционированного доступа обмен данными с камерой может стать невозможным. В этом случае заново выполните подключение с начала.
- Информация аутентификации для подключения к устройству отображается при использовании [Network] – [Network Setup] – [Show Authentication]. Следите за тем, чтобы посторонние лица не видели экран и не могли скопировать изображение QR-кода.
- Имя пользователя и пароль должны быть заданы в момент приобретения. Задавая имя пользователя и пароль, убедитесь, что эти настройки не видно окружающим. Задавайте имя пользователя и пароль следующим образом.

[User Name]	– Задайте имя пользователя, которое включает в себя от 1 до 16 символов. – Его заводская настройка по умолчанию — “admin”. – Ниже указаны допустимые для ввода символы. Буквенные символы (в верхнем и нижнем регистрах), цифровые символы, знаки (! % + , - . = _)
[Password]	– Задайте пароль, который включает в себя от 8 до 16 символов и содержит 1 или более буквенных символов и 1 или более цифровых символов. – Ниже указаны допустимые для ввода символы. Буквенные символы (в верхнем и нижнем регистрах), цифровые символы, знаки (! % + , - . = _)

TP1002221107

MPC-2610
Предупреждения по мерам безопасности

Меры предосторожности в отношении беспроводной ЛВС

В этом разделе рассматриваются меры предосторожности при подключении устройства по беспроводной ЛВС.

- В Справочном руководстве для данного устройства точки доступа беспроводной ЛВС и маршрутизаторы беспроводной ЛВС, которые переключают соединения ЛВС, называются “точки доступа”.
- Для параметра [Security] (способ шифрования) можно задать значение [None], [WPA2] или [WPA3]. С точки зрения безопасности рекомендуется использовать значение [WPA2] или [WPA3]. При выборе [None] перед подключением отображается сообщение. Для безопасности подключения к беспроводной ЛВС настоятельно рекомендуется подключение к точкам доступа с настройкой безопасности WPA2 или WPA3.
- При регистрации точки доступа беспроводной ЛВС с помощью [Manual Register] по умолчанию выбран метод обеспечения безопасности WPA2.
- В случае подключения к точке доступа без какой бы то ни было настройки безопасности можно подвергнуться взлому, доступу злонамеренных третьих лиц или атакам на уязвимости. Если подключение без какой бы то ни было настройки безопасности не является неизбежным, оно не рекомендуется.
- Настройка безопасности беспроводной ЛВС очень важна. Компания Sony не несет ответственности ни за какой ущерб, причиненный несоблюдением мер безопасности, или проблемы безопасности, возникшие вследствие непредотвратимых обстоятельств использования беспроводной ЛВС.

TP1002221108

MPC-2610
Предупреждения по мерам безопасности

Меры предосторожности в отношении тетеринга USB

В этом разделе рассматриваются меры предосторожности при подключении устройства с помощью тетеринга USB.

- Используйте для тетеринга только надежные смартфоны. Подключение к устройствам неизвестного происхождения не рекомендуется из соображений безопасности.

TP1002221109

О функции FTPES (FTPS)

Для обеспечения безопасной передачи файлов функция FTPS поддерживает различные алгоритмы шифрования. Для совместимости с разнообразными серверами поддерживаются многочисленные алгоритмы шифрования, некоторые из которых могут не соответствовать лучшим современным практикам обеспечения безопасности.

Алгоритмы шифрования, поддерживаемые функцией FTPS

Поддерживаются следующие алгоритмы шифрования.

- 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

Рекомендуемые алгоритмы шифрования

На основе рекомендаций Национального института стандартов и технологий США (NIST SP 800-57 Part 1 Revision 5) и соответствующих стандартов безопасности рекомендуются следующие алгоритмы шифрования.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Об алгоритмах, признанных нерекомендуемыми

Для обеспечения совместимости функция FTPS также поддерживает перечисленные ниже алгоритмы, но на основе рекомендаций Национального института стандартов и технологий США (NIST SP 800-57 Part 1 Revision 5) и соответствующих стандартов безопасности они признаны нерекомендуемыми и могут быть исключены в одной из последующих версий.

- 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

О совместимости при соединении

Функция FTPS разработана с соблюдением баланса между безопасностью и совместимостью. В настоящее время по указанным ниже причинам поддерживаются признанные нерекомендуемыми алгоритмы, но они могут быть исключены в одной из последующих версий.

- Внештатным фотографам и видеографам необходимо подключаться к серверам, работающим на различных клиентах.
- Необходимо поддерживать совместимость с более старыми системами и устаревшими серверами.
- Не все пользователи готовы перейти на более безопасную настройку из-за сложности изменения настроек алгоритма шифрования на стороне сервера.
- Настройки FTPS часто совместно используются другими защищенными сервисами. Любые изменения должны быть тщательно обдуманы, так как они могут повлиять на другие сервисы на сервере.
- Чтобы обеспечить возможность взаимодействия в разных средах, должен поддерживаться широкий спектр алгоритмов шифрования.

Используемый во время соединения FTPS алгоритм шифрования определяется путем автоматического согласования с целевым сервером и, следовательно, зависит от настроек сервера. При осознании угроз безопасности приоритет в настоящее время отдается совместимости для удовлетворения разнообразных потребностей пользователей.

Угрозы безопасности

Использование алгоритмов, признанных нерекомендуемыми, в том числе CBC/DHE/RSA/SHA-1, повышает риск расшифровки зашифрованных данных или нарушения их защиты злоумышленниками, что ведет к раскрытию данных во время передачи.

Рекомендации по безопасному подключению

Прежде чем использовать функцию FTPS, убедитесь, что сервер назначения подключения поддерживает рекомендуемый алгоритм шифрования. Включайте на стороне сервера только рекомендуемые алгоритмы, а алгоритмы, признанные нерекомендуемыми, отключайте.

Отправка с использованием безопасного FTP

Файлы можно отправлять с шифрованием, используя для подключения к целевому файловому серверу протокол FTPS в явном режиме (FTPES).
Для безопасной передачи по FTP задайте для параметра [Using Secure Protocol] значение [On] в настройках целевого файлового сервера и импортируйте сертификат.

Справочные материалы

- 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 (с обновлениями по состоянию на 10.06.2016).

Сертификат

Запишите сертификат, используемый функцией FTPES (FTPS), в корневой каталог карты памяти. Задайте следующее имя файла.
certification.pem (формат PEM)
Максимальный раздел отдельного сертификата, который можно загрузить — 1 МБ.