MPC-2610

Środki ostrożności

W niniejszym przewodniku pomocy opisano środki ostrożności związane z transferem plików i przesyłaniem strumieniowym przy użyciu urządzenia.

MPC-2610
Środki ostrożności

Środki ostrożności

W tym temacie opisano zalecenia eksploatacyjne, których należy przestrzegać podczas podłączania urządzenia do sieci.

- Treść komunikacji może być nieświadomie przechwytywana przez nieupoważnione osoby trzecie przebywające w pobliżu sygnałów. W przypadku korzystania z bezprzewodowej komunikacji LAN należy zastosować odpowiednie środki bezpieczeństwa, aby chronić treść komunikacji.
- W przypadku wybrania opcji [None] w ustawieniu [Security] bezprzewodowej sieci LAN i nawiązania połączenia z punktem dostępu komunikacja bezprzewodowa między kamerą i punktem dostępu nie będzie szyfrowana i może zostać przechwycona przez osoby trzecie znajdujące się w zasięgu sygnału. Należy korzystać z protokołu zabezpieczeń WPA2 lub WPA3 w celu zwiększenia bezpieczeństwa.
- FIRMA SONY NIE PONOSI ODPOWIEDZIALNOŚCI ZA JAKIEKOLWIEK SZKODY WYNIKAJĄCE Z NIEZASTOSOWANIA ODPOWIEDNICH ŚRODKÓW ZABEZPIECZAJĄCYCH URZĄDZENIA PRZESYŁOWE, NIEUNIKNIONYCH WYCIEKÓW DANYCH ZGODNYCH ZE SPECYFIKACJĄ TRANSMISJI ANI ZA JAKIEKOLWIEK PROBLEMY ZWIĄZANE Z BEZPIECZEŃSTWEM.
- W zależności od środowiska pracy nieuprawnione osoby trzecie mogą uzyskać dostęp do urządzenia przez sieć. Podczas podłączania urządzenia do sieci należy sprawdzić, czy sieć jest odpowiednio zabezpieczona.
- Po podłączeniu tego produktu do sieci należy nawiązać połączenie za pośrednictwem systemu, który zapewnia funkcje zabezpieczające, takiego jak router lub zapora internetowa. W przypadku połączenia bez takiego zabezpieczenia mogą wystąpić problemy z bezpieczeństwem.

TP1002221089

MPC-2610
Środki ostrożności

Zalecenia eksploatacyjne dotyczące połączenia internetowego

W tym temacie opisano zalecenia eksploatacyjne, których należy przestrzegać podczas podłączania urządzenia do Internetu.

- Urządzenie nie może łączyć się przez bezprzewodową sieć LAN z punktem dostępu używającym tylko metody zabezpieczeń WEP lub WPA, które mają luki w zabezpieczeniach.
- Urządzenie nie jest urządzeniem sieciowym (takim jak router czy przełącznik sieciowy). Zdecydowanie zaleca się połączenie urządzenia z siecią, w której można odpowiednio skonfigurować ustawienia sieciowe i nimi zarządzać w celu ochrony przed atakami sieciowymi, takimi jak ataki typu DoS (Denial of Service).
- W przypadku łączenia urządzenia z siecią należy połączyć je z siecią za pośrednictwem odpowiednio skonfigurowanego i zarządzanego routera lub podłączyć je do portu LAN, który ma taką samą funkcjonalność. W przypadku połączenia bez takiego zabezpieczenia (na przykład podczas korzystania z bezpłatnej sieci Wi-Fi) mogą wystąpić problemy z bezpieczeństwem. Odpowiednio skonfigurowane routery stanowią wystarczające zabezpieczenie przed atakami typu DoS lub utratą funkcjonalności urządzeń w sieci. Po zauważeniu jakichkolwiek nietypowych objawów należy natychmiast odłączyć kamerę od sieci.

TP1002221090

MPC-2610
Środki ostrożności

Zalecenia eksploatacyjne związane z funkcją sieciową

W tym temacie opisano zalecenia eksploatacyjne związane z funkcją sieciową urządzenia.

- W przypadku wykrycia nieautoryzowanego dostępu kamera może nie odbierać komunikacji. W takim przypadku należy ponownie nawiązać połączenie, wykonując procedurę od początku.
- Informacje uwierzytelniające potrzebne do nawiązania połączenia z urządzeniem są wyświetlane podczas korzystania z funkcji [Network] – [Network Setup] – [Show Authentication]. Należy zadbać o to, by inne osoby nie mogły zobaczyć ekranu ani skopiować obrazu kodu QR.
- Bezpośrednio po zakupie konieczne jest ustawienie nazwy użytkownika i hasła. Podczas ustawiania własnej nazwy użytkownika i hasła należy upewnić się, że ustawienia te nie są widoczne dla innych osób. Nazwę użytkownika i hasło należy ustawić w następujący sposób.

[User Name]	– Należy ustawić nazwę użytkownika składającą się z 1–16 znaków. – Domyślne ustawienie fabryczne to „admin”. – Prawidłowe znaki wejściowe podano poniżej. Znaki alfabetu (małe i wielkie litery), znaki numeryczne, symbole (! % + , - . = _)
[Password]	– Należy ustawić hasło składające się z 8–16 znaków, zawierające co najmniej 1 znak alfabetyczny i co najmniej 1 znak numeryczny. – Prawidłowe znaki wejściowe podano poniżej. Znaki alfabetu (małe i wielkie litery), znaki numeryczne, symbole (! % + , - . = _)

TP1002221091

MPC-2610
Środki ostrożności

Zalecenia eksploatacyjne dotyczące bezprzewodowej sieci LAN

W tym temacie opisano zalecenia eksploatacyjne, których należy przestrzegać podczas podłączania urządzenia za pośrednictwem bezprzewodowej sieci LAN.

- W przewodniku pomocy dotyczącym tego urządzenia punkty dostępu do bezprzewodowej sieci LAN i routery bezprzewodowej sieci LAN, które przekazują połączenia LAN, są określane jako „punkty dostępu”.
- Opcję [Security] (metoda szyfrowania) można ustawić na [None], [WPA2] lub [WPA3]. Korzystanie z ustawienia [WPA2] lub [WPA3] jest zalecane z punktu widzenia bezpieczeństwa. Jeśli jest wybrana opcja [None], przed nawiązaniem połączenia wyświetlany jest komunikat. W celu zapewnienia bezpiecznego połączenia z bezprzewodową siecią LAN zdecydowanie zalecane jest połączenie z punktami dostępu z ustawieniami zabezpieczeń WPA2 lub WPA3.
- Podczas rejestrowania punktu dostępu do bezprzewodowej sieci LAN przy użyciu opcji [Manual Register] domyślnie wybrana jest metoda zabezpieczeń WPA2.
- W przypadku połączenia z punktem dostępu bez żadnych ustawień zabezpieczeń użytkownik może być narażony na ataki hakerskie, uzyskanie dostępu przez osoby o złośliwych intencjach lub ataki wykorzystujące luki w zabezpieczeniach. Jeśli nie jest to absolutnie konieczne, nie zaleca się nawiązywania połączeń bez żadnych ustawień zabezpieczeń.
- Skonfigurowanie zabezpieczeń bezprzewodowej sieci LAN jest bardzo istotne. Firma Sony nie ponosi odpowiedzialności za jakiekolwiek szkody wynikające z niepodjęcia środków bezpieczeństwa lub wystąpienia problemu związanego z bezpieczeństwem podczas korzystania z bezprzewodowej sieci LAN z powodu okoliczności, których nie można uniknąć.

TP1002221092

MPC-2610
Środki ostrożności

Zalecenia eksploatacyjne dotyczące tetheringu przez USB

W tym temacie opisano zalecenia eksploatacyjne, których należy przestrzegać podczas podłączania urządzenia za pomocą funkcji tetheringu przez USB.

- Do tetheringu należy używać tylko zaufanych urządzeń typu smartfon. Nawiązywanie połączeń z nieznanymi urządzeniami nie jest zalecane ze względów bezpieczeństwa.

TP1002221093

MPC-2610
Środki ostrożności

Informacje o funkcji FTPES (FTPS)

Funkcja FTPS obsługuje różne algorytmy szyfrowania w celu zapewnienia bezpiecznego transferu plików. Aby zapewnić kompatybilność z wieloma różnymi serwerami, obsługiwanych jest wiele algorytmów szyfrowania, jednak niektóre mogą być niezgodne z obecnie obowiązującymi najlepszymi praktykami w zakresie zabezpieczeń.

Algorytmy szyfrowania obsługiwane przez funkcję FTPS

Obsługiwane są następujące algorytmy szyfrowania.

- 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

Zalecane algorytmy szyfrowania

Następujące algorytmy szyfrowania są zalecane na podstawie zaleceń NIST (NIST SP 800-57 Part 1 Revision 5) i powiązanych norm w zakresie zabezpieczeń.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Informacje o przestarzałych algorytmach

Funkcja FTPS obsługuje także poniższe algorytmy w celu zapewnienia kompatybilności, ale są one uznawane za przestarzałe w oparciu o zalecenia NIST (NIST SP 800-57 Part 1 Revision 5) oraz powiązanych norm w zakresie zabezpieczeń i mogą zostać usunięte w przyszłej wersji.

- 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

Informacje o kompatybilności połączeń

Funkcja FTPS została zaprojektowana z zachowaniem równowagi między bezpieczeństwem i kompatybilnością. Obecnie przestarzałe algorytmy są obsługiwane z podanych poniżej powodów, ale mogą zostać usunięte w przyszłej wersji w celu zwiększenia bezpieczeństwa.

- Niezależni fotografowie i kamerzyści muszą łączyć się z serwerami działającymi w różnych systemach klienckich.
- Dlatego ważne jest zachowanie kompatybilności ze starszymi systemami i serwerami.
- Nie wszyscy użytkownicy są gotowi na zmianę ustawień na bardziej bezpieczne, ponieważ zmiana ustawień algorytmu szyfrowania po stronie serwera jest skomplikowanym zadaniem.
- Ustawienia FTPS są często współdzielone z innymi bezpiecznymi usługami. Należy starannie rozważyć wszelkie zmiany, ponieważ mogą mieć one wpływ na inne usługi na serwerze.
- W celu zapewnienia interoperacyjności w różnych środowiskach musi być obsługiwany szeroki zakres algorytmów szyfrowania.

Algorytm szyfrowania używany podczas połączenia FTPS jest określany poprzez automatyczną negocjację z serwerem docelowym i dlatego zależy od ustawień serwera. Zdajemy sobie sprawę z zagrożeń bezpieczeństwa, ale kompatybilność jest obecnie traktowana priorytetowo, aby zaspokoić różnorodne potrzeby użytkowników.

Zagrożenia bezpieczeństwa

Korzystanie z przestarzałych algorytmów, w tym CBC/DHE/RSA/SHA-1, zwiększa ryzyko, że zaszyfrowane dane mogą zostać odszyfrowane lub zmodyfikowane przez osobę dokonującą ataku, przez co może dojść do naruszenia bezpieczeństwa danych podczas przesyłania.

Zalecenie dotyczące bezpiecznego połączenia

Przed przystąpieniem do korzystania z funkcji FTPS należy sprawdzić, czy serwer docelowy połączenia obsługuje zalecany algorytm szyfrowania. Po stronie serwera należy włączyć tylko zalecane algorytmy i wyłączyć przestarzałe.

Przesyłanie za pomocą bezpiecznego protokołu FTP

Możesz przesyłać pliki z szyfrowaniem, korzystając z FTPS w trybie jawnym (FTPES) do połączenia z docelowym serwerem plików.
Aby włączyć bezpieczny transfer przy użyciu protokołu FTP, ustaw opcję [Using Secure Protocol] na [On] w ustawieniach docelowego serwera transferu plików i zaimportuj certyfikat.

Odwołania

- 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 (obejmuje aktualizacje z dnia 10/06/2016).

Certyfikat

Certyfikat używany przez funkcję FTPES (FTPS) należy zapisać w katalogu głównym karty pamięci. Nazwę pliku należy ustawić następująco:
certification.pem (format PEM)
Maksymalny rozmiar certyfikatu, który można wczytać, to 1 MB na każdy certyfikat.

TP1002221094