MPC-2610

Precauzioni per la sicurezza

Questa Guida descrive le precauzioni per la sicurezza per il trasferimento di file e lo streaming con l’unità.

MPC-2610
Precauzioni per la sicurezza

Precauzioni per la sicurezza

Questo argomento descrive le precauzioni relative al collegamento dell’unità a una rete.

- Il contenuto trasmesso può essere intercettato da terze parti non autorizzate che si trovano in prossimità dei segnali senza la conoscenza dell’utente. Quando si utilizza la modalità di comunicazione LAN wireless, implementare adeguate misure di sicurezza per proteggere il contenuto della comunicazione.
- Se l’impostazione [Security] per la LAN wireless è configurata su [None] e si collega la telecamera a un punto di accesso, la comunicazione wireless fra la telecamera e tale punto di accesso non sarà crittografata e potrà essere intercettata da terze parti eventualmente presenti nel campo di propagazione del segnale. Utilizzare i protocolli di sicurezza WPA2 o WPA3 per una maggiore sicurezza.
- SONY NON SARÀ RESPONSABILE PER DANNI DI QUALSIASI TIPO RISULTANTI DALLA MANCATA IMPLEMENTAZIONE DI ADEGUATE MISURE DI SICUREZZA SUI DISPOSITIVI DI TRASMISSIONE, DA INEVITABILI PERDITE O FUGHE DI DATI RISULTANTI DALLE SPECIFICHE TECNICHE DELLA TRASMISSIONE O DA PROBLEMATICHE RELATIVE ALLA SICUREZZA DI QUALSIASI TIPO.
- A seconda dell’ambiente operativo, il sistema potrebbe risultare accessibile in rete a terzi non autorizzati. Prima di collegare l’apparecchio in rete, assicurarsi che la rete sia protetta in modo sicuro.
- Il collegamento del prodotto a una rete deve essere realizzato mediante un sistema in grado di fornire funzioni di protezione, ad esempio un router o un firewall. In caso di collegamento senza tale protezione si potrebbero verificare problemi di sicurezza.

TP1002221001

MPC-2610
Precauzioni per la sicurezza

Precauzioni per collegamento a Internet

Questo argomento descrive le precauzioni relative al collegamento dell’unità a Internet.

- L’unità non è in grado di connettersi tramite LAN wireless a un punto di accesso che utilizza solo i protocolli WEP o WPA. Tali protocolli presentano infatti vulnerabilità per quanto riguarda la sicurezza.
- L’unità non è un dispositivo di rete (ad esempio, un router o uno switch). Si consiglia vivamente di collegare l’unità a una rete di cui sia possibile configurare e gestire le impostazioni in modo appropriato per proteggersi da attacchi provenienti dalla rete stessa, ad esempio attacchi DoS (attacchi Denial of Service).
- Per il collegamento dell’unità a una rete, servirsi di un router opportunamente configurato e gestito, oppure utilizzare una porta LAN dotata di analoghe funzionalità. Se il collegamento avviene senza tali protezioni (ad esempio nel caso di Wi-Fi aperti a tutti), potrebbero verificarsi problemi di sicurezza. Se configurati correttamente, i router forniscono una protezione sufficiente contro gli attacchi DoS o la perdita di funzionalità dei dispositivi nella rete. Se si nota qualcosa di insolito, scollegare immediatamente la telecamera dalla rete.

TP1002221002

MPC-2610
Precauzioni per la sicurezza

Precauzioni relative alla funzione di rete

Questo argomento descrive le precauzioni relative alla funzione di rete dell’unità.

- Se viene rilevato un accesso non autorizzato, la telecamera potrebbe interrompere la ricezione di comunicazioni. In questo caso, ripetere la procedura di connessione dall’inizio.
- Quando si utilizza [Network] – [Network Setup] – [Show Authentication] vengono visualizzate le informazioni di autenticazione per la connessione all'unità. Assicurarsi che la schermata non possa essere vista e che l’immagine del codice QR non possa essere copiata da altri.
- Al momento dell'acquisto è necessario impostare un nome utente e una password. Quando si imposta il nome utente e la password, assicurarsi che tali impostazioni non siano visibili a terzi. Impostare il nome utente e la password come descritto di seguito.

[User Name]	– Impostare un nome utente composto da 1 a 16 caratteri. – L’impostazione predefinita è “admin”. – Di seguito sono riportati i caratteri validi consentiti. Caratteri alfabetici (maiuscole e minuscole), caratteri numerici, simboli (! % + , - . = _)
[Password]	– Impostare una password composta da 8 a 16 caratteri contenenti almeno 1 o più caratteri alfabetici e 1 o più caratteri numerici. – Di seguito sono riportati i caratteri validi consentiti. Caratteri alfabetici (maiuscole e minuscole), caratteri numerici, simboli (! % + , - . = _)

TP1002221003

MPC-2610
Precauzioni per la sicurezza

Precauzioni relative alla LAN wireless

Questo argomento descrive le precauzioni relative al collegamento dell’unità tramite una LAN wireless.

- Nella Guida di questa unità, i punti di accesso LAN wireless e i router LAN wireless che inoltrano le connessioni LAN vengono definiti “punti di accesso”.
- [Security] (metodo di crittografia) può essere impostato su [None], [WPA2] o [WPA3]. Dal punto di vista della sicurezza, è consigliabile l’uso di [WPA2] o [WPA3]. Quando è selezionato [None], prima della connessione viene visualizzato un messaggio. Per garantire una connessione LAN wireless sicura, si consiglia vivamente di connettersi a punti di accesso protetti con impostazione di sicurezza WPA2 o WPA3.
- Quando si registra un punto di accesso LAN wireless utilizzando [Manual Register], il metodo di sicurezza WPA2 è selezionato per impostazione predefinita.
- La connessione a punti di accesso senza nessuna impostazione di sicurezza potrebbe permettere hacking, accesso da parte di terzi malintenzionati o attacchi a vulnerabilità eventualmente presenti. A meno che non sia assolutamente inevitabile, la connessione senza alcuna impostazione di sicurezza non è mai consigliata.
- La configurazione della sicurezza su una LAN wireless è molto importante. Sony non potrà essere ritenuta responsabile per eventuali danni derivanti dalla mancata adozione di misure di sicurezza o nel caso in cui si verifichi un problema di sicurezza a causa di circostanze inevitabili nell’uso della LAN wireless.

TP1002221004

MPC-2610
Precauzioni per la sicurezza

Precauzioni relative al tethering USB

Questo argomento descrive le precauzioni relative al collegamento dell’unità tramite tethering USB.

- Per il tethering, utilizzare solo smartphone di cui si ha fiducia. La connessione a dispositivi di origine sconosciuta non è consigliata per motivi di sicurezza.

TP1002221005

Informazioni sulla funzione FTPES (FTPS)

La funzione FTPS supporta vari algoritmi di crittografia per garantire un trasferimento sicuro dei file. Per consentire la compatibilità con un'ampia gamma di server, sono supportati molti algoritmi di crittografia, alcuni dei quali potrebbero non essere conformi alle procedure consigliate per la sicurezza correnti.

Algoritmi di crittografia supportati dalla funzione FTPS

Sono supportati i seguenti algoritmi di crittografia:

- 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

Algoritmi di crittografia raccomandati

In base alle raccomandazioni NIST (NIST SP 800-57 Parte 1 Revisione 5) e agli standard di sicurezza correlati, sono raccomandati i seguenti algoritmi di crittografia:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Informazioni sugli algoritmi deprecati

Per motivi di compatibilità, la funzione FTPS supporta anche i seguenti algoritmi. Tali algoritmi, tuttavia, sono deprecati in base alle raccomandazioni NIST (NIST SP 800-57 Parte 1 Revisione 5) e agli standard di sicurezza correlati e potrebbero essere rimossi in una versione futura.

- 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

Informazioni sulla compatibilità delle connessioni

La funzione FTPS è concepita per offrire un equilibrio tra sicurezza e compatibilità. Attualmente, gli algoritmi deprecati sono supportati per i motivi descritti di seguito, ma tali algoritmi potrebbero essere rimossi in una versione futura per migliorare la sicurezza.

- I fotografi e i videografi freelance devono potersi connettersi a server in esecuzione su una vasta gamma di client.
- È necessario mantenere la compatibilità con i sistemi più vecchi e i server legacy.
- Non tutti gli utenti sono disposti a passare a un'impostazione più sicura perché la modifica delle impostazioni dell'algoritmo di crittografia sul lato server è complicata.
- Le impostazioni FTPS sono spesso condivise con altri servizi sicuri. Tutte le eventuali modifiche devono essere considerate attentamente in quanto potrebbero avere un impatto su altri servizi sul server.
- È necessario supportare un'ampia gamma di algoritmi di crittografia per garantire l'interoperabilità in ambienti diversi.

L'algoritmo di crittografia utilizzato durante una connessione FTPS è determinato dalla negoziazione automatica con il server di destinazione e quindi dipende dalle impostazioni del server stesso. Pur essendo consapevoli dei rischi per la sicurezza, viene attualmente data maggior importanza alla compatibilità per soddisfare le diverse esigenze degli utenti.

Rischi per la sicurezza

L'utilizzo di algoritmi deprecati, tra cui CBC/DHE/RSA/SHA-1, aumenta il rischio che i dati crittografati possano essere decrittati o manomessi da malintenzionati, esponendo tali dati durante il trasferimento.

Raccomandazione per la sicurezza della connessione

Prima di utilizzare la funzione FTPS, verificare che il server di destinazione della connessione supporti un algoritmo di crittografia raccomandato. Abilitare solo gli algoritmi raccomandati sul lato server e disabilitare gli algoritmi deprecati.

Upload tramite Secure FTP

È possibile proteggere con crittografia l'upload dei file utilizzando il protocollo FTPS in modalità Explicit (FTPES) per realizzare la connessione con il file server di destinazione.
Per utilizzare il protocollo Secure FTP, impostare [Using Secure Protocol] su [On] nelle impostazioni del file server di destinazione del trasferimento e importarne il relativo certificato.

Riferimenti

- 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 (include aggiornamenti a partire dal 10/06/2016).

Certificato

Scrivere il certificato utilizzato dalla funzione FTPES (FTPS) nella directory radice di una scheda di memoria. Impostare il nome del file come segue.
certification.pem (formato PEM)
Possono essere caricati solo certificati le cui dimensioni non superino 1 MB.

TP1002221006