SONY

Ghid de asistență

MPC-2610

Măsuri de precauţie pentru securitate

Acest Ghid de asistență descrie măsurile de precauție pentru securitate pentru transferul de fișiere și streaming utilizând unitatea.

MPC-2610
Măsuri de precauţie pentru securitate

Măsuri de precauţie pentru securitate

Acest subiect descrie măsurile de precauție la conectarea unității la o rețea.

- Conținutul comunicației poate fi interceptat fără intenție de către terți neautorizați aflați în apropierea semnalelor. Atunci când utilizați comunicații LAN fără fir, implementați măsuri de securitate adecvate, pentru a proteja conținutul comunicării.
- Dacă stabiliți setarea [Security] pentru LAN fără fir la [None] și vă conectați la un punct de acces, comunicarea fără fir dintre cameră și punctul de acces nu va fi criptată și poate fi interceptată de o terță parte, aflată în raza de acțiune a semnalului. Utilizați protocolul de securitate WPA2 sau WPA3 pentru un plus de securitate.
- COMPANIA SONY NU VA FI RESPONSABILĂ PENTRU PAGUBELE DE ORICE FEL DETERMINATE DE NEAPLICAREA CORECTĂ A MĂSURILOR DE SECURITATE PRIVIND DISPOZITIVELE DE TRANSMISIE, PIERDERI INEVITABILE DE DATE PROVOCATE DE SPECIFICAŢIILE DE TRANSMISIE SAU PROBLEME DE SECURITATE DE ORICE FEL.
- În funcţie de mediul de funcţionare, terţi neautorizaţi din reţea pot accesa unitatea. Când conectaţi unitatea la reţea, verificaţi dacă reţeaua este bine protejată.
- Atunci când conectați acest produs la o rețea, conectați-l printr-un sistem care oferă o funcție de protecție, cum ar fi un router sau un firewall. Dacă se realizează conexiunea fără o astfel de protecție, pot apărea probleme de securitate.

TP1002221049

MPC-2610
Măsuri de precauţie pentru securitate

Măsuri de precauţie privind conexiunea la Internet

Acest subiect descrie măsurile de precauție la conectarea unității la internet.

- Unitatea nu se poate conecta prin LAN fără fir la un punct de acces care utilizează doar WEP sau WPA, care sunt metode de securitate cu vulnerabilități.
- Unitatea nu este un dispozitiv de rețea (de exemplu, un router sau un hub de comutare). Se recomandă insistent conectarea unității la o rețea, unde puteți configura și gestiona setările de rețea în mod adecvat, pentru a proteja împotriva atacurilor bazate pe rețea, cum ar fi atacurile DoS (atacuri de tip refuzul serviciului).
- Când conectați unitatea la o rețea, conectați-o prin intermediul unui router configurat și gestionat în mod corespunzător sau conectați-o la un port LAN cu aceeași funcționalitate. Dacă unitatea este conectată fără o astfel de protecție (de exemplu, când utilizați Wi-Fi gratuit), pot apărea probleme de securitate. Când sunt configurate corespunzător, routerele oferă protecție suficientă împotriva atacurilor DoS sau a pierderii funcționalității dispozitivelor din rețea. Dacă observați ceva neobișnuit, deconectați imediat camera de la rețea.

TP1002221050

MPC-2610
Măsuri de precauţie pentru securitate

Măsuri de precauţie legate de funcția de rețea

Acest subiect descrie măsurile de precauție privind funcția de rețea a unității.

- Dacă este detectat un acces neautorizat, camera poate deveni incapabilă să accepte comunicații. Dacă acest lucru se întâmplă, reconectați de la început.
- Informațiile de autentificare pentru conectarea la unitate sunt afișate atunci când utilizați [Network] – [Network Setup] – [Show Authentication]. Aveți grijă ca ecranul să nu poată fi vizualizat și ca imaginea codului QR să nu poată fi copiată de alte persoane.
- În momentul achiziției, trebuie să configurați un nume de utilizator și o parolă. Atunci când vă setați numele de utilizator și parola, asigurați-vă că setările nu sunt vizibile pentru alte persoane. Setați numele de utilizator și parola după cum urmează.

[User Name]	– Setați un nume de utilizator care să conțină între 1 și 16 caractere. – În mod implicit, din fabrică, acesta este „admin”. – Puteți introduce următoarele caractere valabile. Caractere alfabetice (majuscule și litere mici), caractere numerice, simboluri (! % + , - . = _)
[Password]	– Setați o parolă care să conțină între 8 și 16 caractere, cu cel puțin 1 sau mai multe caractere alfabetice și 1 sau mai multe caractere numerice. – Puteți introduce următoarele caractere valabile. Caractere alfabetice (majuscule și litere mici), caractere numerice, simboluri (! % + , - . = _)

TP1002221051

MPC-2610
Măsuri de precauţie pentru securitate

Măsuri de precauţie legate de LAN fără fir

Acest subiect descrie măsurile de precauție la conectarea unității prin LAN fără fir.

- În Ghidul de asistență pentru această unitate, punctele de acces LAN fără fir și routerele LAN fără fir care retransmit conexiunile LAN sunt denumite „puncte de acces”.
- [Security] (metodă de criptare) poate fi setată la [None], [WPA2] sau la [WPA3]. Utilizarea [WPA2] sau [WPA3] este recomandată din punct de vedere al securității. Când este selectat [None], înainte de conectare se afișează un mesaj. Pentru o conexiune LAN wireless sigură, se recomandă cu insistență conectarea la puncte de acces cu setările de securitate WPA2 sau WPA3.
- În mod implicit, este selectată metoda de securitate WPA2 atunci când se înregistrează un punct de acces LAN wireless prin [Manual Register].
- Dacă vă conectați la un punct de acces fără nicio setare de securitate, puteți fi supus pirateriei informatice, accesului de către părți terțe rău intenționate sau atacurilor asupra punctelor vulnerabile. Cu excepția cazului în care este inevitabil, nu se recomandă conectarea fără nicio setare de securitate.
- Configurarea securității pe o rețea LAN fără fir este foarte importantă. Sony nu va fi răspunzătoare pentru niciun prejudiciu rezultat din neadoptarea măsurilor de securitate sau dacă apare o problemă de securitate din cauza unor circumstanțe inevitabile în utilizarea LAN fără fir.

TP1002221052

MPC-2610
Măsuri de precauţie pentru securitate

Măsuri de precauţie aferente partajării conexiunii USB

Acest subiect descrie măsurile de precauție la conectarea unității prin partajarea conexiunii USB.

- Utilizați doar dispozitive smartphone de încredere pentru partajarea conexiunii. Conectarea la dispozitive de origine necunoscută nu este recomandată, din cauza problemelor legate de securitate.

TP1002221053

Despre funcția FTPES (FTPS)

Funcția FTPS acceptă diverși algoritmi de criptare pentru a asigura transferul securizat de fișiere. Mai mulți algoritmi de criptare, dintre care este posibil ca unii să nu respecte cele mai bune practici actuale de securitate, sunt acceptați pentru compatibilitate cu o gamă largă de servere.

Algoritmi de criptare acceptați de funcția FTPS

Următorii algoritmi de criptare sunt acceptați.

- 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 de criptare recomandați

Următorii algoritmi de criptare sunt recomandați pe baza recomandărilor NIST (NIST SP 800-57 partea 1 versiunea 5) și a standardelor conexe de securitate.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Despre algoritmi depășiți

Funcția FTPS acceptă, de asemenea, următorii algoritmi pentru compatibilitate, dar aceștia sunt depreciați conform recomandărilor NIST (NIST SP 800-57 partea 1 versiunea 5) și a standardelor conexe de securitate și pot fi eliminați într-o versiune viitoare.

- 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

Despre compatibilitatea conexiunii

Funcția FTPS este concepută ca un echilibru între securitate și compatibilitate. În prezent, algoritmii depreciați sunt acceptați din următoarele motive, dar pot fi eliminați într-o versiune viitoare, pentru a îmbunătăți securitatea.

- Fotografii și videografii liber profesioniști trebuie să se conecteze la servere care rulează pe diverși clienți.
- Compatibilitatea cu sistemele mai vechi și serverele existente trebuie menținută.
- Nu toți utilizatorii sunt pregătiți să treacă la o setare mai sigură, deoarece modificarea setărilor algoritmilor de criptare pe partea de server este complicată.
- Setările FTPS sunt deseori partajate cu alte servicii securizate. Orice modificări trebuie analizate cu atenție, deoarece pot avea impact asupra altor servicii de pe server.
- Este necesară compatibilitatea cu o gamă largă de algoritmi de criptare, pentru a asigura interoperabilitatea în diferite medii.

Algoritmul de criptare utilizat în timpul unei conexiuni FTPS este determinat prin negociere automată cu serverul de destinație și, prin urmare, depinde de setările serverului. Deși riscurile de securitate sunt cunoscute, compatibilitatea are prioritate, pentru a satisface diversele nevoi ale utilizatorilor.

Riscuri de securitate

Utilizarea algoritmilor depreciați, inclusiv CBC/DHE/RSA/SHA-1, mărește riscul ca datele criptate să fie decriptate sau modificate de un atacator, expunând datele în timpul transferului.

Recomandare de conexiune securizată

Înainte de a utiliza funcția FTPS, verificați dacă serverul de destinație al conexiunii acceptă algoritmul de criptare recomandat. Activați doar algoritmii recomandați pe partea serverului și dezactivați algoritmii depreciați.

Încărcarea prin FTP securizat

Puteți încărca fișiere cu criptare folosind FTPS în modul explicit (FTPES) pentru conectarea cu serverul de destinație pentru fișiere.
Pentru un transfer FTP securizat, configurați [Using Secure Protocol] la [On] în setările serverului de destinație pentru transferul de fișiere și importați un certificat.

Referințe

- 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 actualizări până la 10.06.2016).

Certificat

Scrieți certificatul utilizat de funcția FTPES (FTPS) în directorul rădăcină al unui card de memorie. Setați numele fișierului după cum urmează.
certification.pem (format PEM)
Dimensiunea maximă a certificatului care poate fi încărcată este de 1 MB per certificat.

TP1002221054