MPC-2610

Veiligheidsmaatregelen

Deze Help-gids beschrijft de veiligheidsmaatregelen voor bestandsoverdracht en streaming met behulp van het apparaat.

MPC-2610
Veiligheidsmaatregelen

Veiligheidsmaatregelen

Dit onderwerp beschrijft de veiligheidsmaatregelen bij het verbinden van het apparaat met een netwerk.

- De inhoud van communicatie kan zonder dat u dat weet worden onderschept door onbevoegden in de buurt van het signaal. Wanneer u draadloze LAN-communicatie gebruikt, pas dan correcte beveiligingsmaatregelen toe om de inhoud van uw communicatie te beschermen.
- Als u de instelling voor [Security] draadloos LAN instelt op [None] en met een toegangspunt verbinding maakt, is de draadloze communicatie tussen de camera en het toegangspunt niet versleuteld en kan deze worden onderschept door derden die zich binnen het bereik van het signaal bevinden. Gebruik het beveiligingsprotocol WPA2 of WPA3 voor een betere beveiliging.
- SONY IS NIET AANSPRAKELIJK VOOR WELKE SCHADE DAN OOK DIE VOORTKOMT UIT HET NIET NEMEN VAN VOLDOENDE BEVEILIGINGSMAATREGELEN OP TRANSMISSIEAPPARATEN, ONVERMIJDBARE GEGEVENSLEKKEN DOOR TRANSMISSIESPECIFICATIES OF BEVEILIGINGSPROBLEMEN VAN WELKE AARD DAN OOK.
- Afhankelijk van de gebruiksomgeving kunnen onbevoegden via het netwerk toegang krijgen tot het apparaat. Wanneer u het apparaat verbinding laat maken met het netwerk, zorg er dan voor dat het netwerk goed is beveiligd.
- Wanneer u dit product aansluit op een netwerk, maak dan verbinding via een systeem dat beveiliging biedt, zoals een router of firewall. Als u verbinding maakt zonder dergelijke bescherming kunnen beveiligingsproblemen ontstaan.

TP1002220968

MPC-2610
Veiligheidsmaatregelen

Voorzorgsmaatregelen voor internetverbinding

Dit onderwerp beschrijft de voorzorgsmaatregelen bij het verbinden van het apparaat met het internet.

- Het apparaat kan niet via een draadloos LAN met een toegangspunt verbinden dat alleen WEP of WPA gebruikt. Dat zijn beveiligingsmethodes die kwetsbaarheden vertonen.
- Het apparaat is geen netwerkapparaat (bijvoorbeeld een router of switchhub). Het wordt ten zeerste aangeraden om het apparaat met een netwerk te verbinden, waar u de netwerkinstellingen op de juiste manier kunt configureren en beheren om u tegen netwerkaanvallen, zoals DoS-aanvallen (Denial-of-Service-aanvallen), te beschermen.
- Verbind het apparaat bij het verbinden met een netwerk via een router die op de juiste manier is geconfigureerd en wordt beheerd of verbind het met een LAN-poort met dezelfde functionaliteit. Als er verbinding wordt gemaakt zonder een dergelijke bescherming (bijvoorbeeld bij gebruik van gratis wifi), kunnen er beveiligingsproblemen optreden. Indien goed geconfigureerd, bieden routers voldoende bescherming tegen DoS-aanvallen of verlies van functionaliteit bij apparaten in het netwerk. Als u iets ongewoon opmerkt, koppel de camera dan onmiddellijk los van het netwerk.

TP1002220969

MPC-2610
Veiligheidsmaatregelen

Voorzorgsmaatregelen met betrekking tot de netwerkfunctie

Dit onderwerp beschrijft de voorzorgsmaatregelen met betrekking tot de netwerkfunctie van het apparaat.

- Als er onbevoegde toegang wordt gedetecteerd, kan de camera mogelijk geen communicatie meer aanvaarden. Als dit gebeurt, maak dan opnieuw verbinding vanaf het begin.
- De authenticatie-informatie voor verbinding wordt weergegeven wanneer u [Network] – [Network Setup] – [Show Authentication] gebruikt. Zorg dat het scherm niet bekeken kan worden en dat de QR code afbeelding niet gekopieerd kan worden door anderen.
- Op het moment van aankoop moet een gebruikersnaam en wachtwoord worden ingesteld. Zorg er bij het instellen van uw gebruikersnaam en wachtwoord voor dat anderen de instellingen niet kunnen zien. Stel de gebruikersnaam en het wachtwoord als volgt in.

[User Name]	– Stel een gebruikersnaam in van 1 tot 16 tekens. – Dit is standaard ingesteld op "admin". – De volgende tekens zijn geldige invoertekens. Alfabetische tekens (hoofdletters en kleine letters), numerieke tekens, symbolen (! % + , - . = _)
[Password]	– Stel een wachtwoord in van 8 tot 16 tekens met ten minste 1 of meer alfabetische tekens en 1 of meer numerieke tekens. – De volgende tekens zijn geldige invoertekens. Alfabetische tekens (hoofdletters en kleine letters), numerieke tekens, symbolen (! % + , - . = _)

TP1002220970

MPC-2610
Veiligheidsmaatregelen

Voorzorgsmaatregelen met betrekking tot draadloos LAN

Dit onderwerp beschrijft de voorzorgsmaatregelen bij het verbinden van het apparaat met draadloos LAN.

- In de Help-gids voor dit apparaat worden draadloze LAN-toegangspunten en draadloze LAN-routers die LAN-verbindingen doorsturen "toegangspunten" genoemd.
- [Security] (versleutelingsmethode) kan worden ingesteld op [None], [WPA2] of [WPA3]. Het gebruik van [WPA2] of [WPA3] wordt vanuit beveiligingsoogpunt aanbevolen. Wanneer [None] is geselecteerd, wordt een bericht weergegeven voordat verbinding wordt gemaakt. Voor een veilige draadloze LAN-verbinding wordt verbinding met toegangspunten met een WPA2- of WPA3-beveiligingsinstelling sterk aanbevolen.
- Standaard wordt de beveiligingsmethode WPA2 geselecteerd wanneer een draadloos LAN-toegangspunt wordt geregistreerd met [Manual Register].
- Als u met een toegangspunt verbinding maakt zonder enige beveiligingsinstelling, kunt u worden blootgesteld aan hacken, toegang door kwaadwillende derden of aanvallen op kwetsbaarheden. Tenzij het onvermijdelijk is, wordt een verbinding zonder beveiligingsinstellingen niet aanbevolen.
- Het instellen van beveiliging op een draadloos LAN is heel belangrijk. Sony is niet aansprakelijk voor schade als gevolg van het niet nemen van beveiligingsmaatregelen of als er een beveiligingsprobleem optreedt als gevolg van onvermijdelijke omstandigheden bij het gebruik van draadloos LAN.

TP1002220971

MPC-2610
Veiligheidsmaatregelen

Voorzorgsmaatregelen met betrekking tot USB-tethering

Dit onderwerp beschrijft de voorzorgsmaatregelen bij het verbinden van het apparaat via USB-tethering.

- Gebruik alleen vertrouwde smartphones voor tethering. Verbinden met apparaten van onbekende herkomst wordt afgeraden vanwege beveiligingsrisico's.

TP1002220972

Over de FTPES (FTPS)-functie

De FTPS-functie ondersteunt verschillende versleutelingsalgoritmes om een veilige bestandsoverdracht te garanderen. Verschillende versleutelingsalgoritmes, waarvan sommige mogelijk niet voldoen aan de huidige beste praktijken voor beveiliging, worden ondersteund voor compatibiliteit met een breed scala van servers.

Versleutelingsalgoritmes ondersteund door de FTPS-functie

De volgende versleutelingsalgoritmes worden ondersteund.

- 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

Aanbevolen versleutelingsalgoritmes

De volgende versleutelingsalgoritmes worden aanbevolen op basis van de NIST-aanbevelingen (NIST SP 800-57 Deel 1 Revisie 5) en gerelateerde beveiligingsstandaarden.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Over verouderde algoritmes

De FTPS-functie ondersteunt ook de volgende algoritmes voor compatibiliteit, maar deze zijn verouderd op basis van de NIST-aanbevelingen (NIST SP 800-57 Deel 1 Revisie 5) en gerelateerde beveiligingsstandaarden en worden mogelijk in een toekomstige versie verwijderd.

- 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

Over verbindingscompatibiliteit

De FTPS-functie is ontworpen met een evenwicht tussen beveiliging en compatibiliteit. Momenteel worden verouderde algoritmen ondersteund om volgende redenen, maar deze worden in een toekomstige versie mogelijk verwijderd om de beveiliging te verbeteren.

- Freelance fotografen en videografen moeten verbinding maken met servers die op verschillende clients draaien.
- Compatibiliteit met oudere systemen en verouderde servers moet onderhouden worden.
- Niet alle gebruikers zijn bereid om over te stappen op veiligere instellingen, omdat het wijzigen van de instellingen van versleutelingsalgoritmes aan de serverkant ingewikkeld is.
- De FTPS-instellingen worden vaak gedeeld met andere beveiligde diensten. Eventuele wijzigingen moeten zorgvuldig worden overwogen, omdat ze van invloed kunnen zijn op andere diensten op de server.
- Er moet een breed scala aan versleutelingsalgoritmes worden ondersteund om interoperabiliteit in verschillende omgevingen te garanderen.

Het versleutelingsalgoritme dat wordt gebruikt tijdens een FTPS-verbinding wordt bepaald door automatische onderhandeling met de bestemmingsserver en is daarom van de serverinstellingen afhankelijk. Hoewel wij ons bewust zijn van de beveiligingsrisico's, wordt op dit moment voorrang gegeven aan compatibiliteit om aan de uiteenlopende behoeften van gebruikers te voldoen.

Beveiligingsrisico's

Het gebruik van verouderde algoritmes, waaronder CBC/DHE/RSA/SHA-1, vergroot het risico dat versleutelde gegevens worden ontsleuteld en gemanipuleerd door een aanvaller, waardoor er tijdens het overdragen toegang is tot gegevens.

Aanbevelingen voor beveiligde verbinding

Controleer voordat u de FTPS-streamingfunctie gebruikt of de bestemmingsserver van de verbinding het aanbevolen versleutelingsalgoritme ondersteunt. Schakel alleen de aanbevolen algoritmes aan de serverkant in en schakel de verouderde algoritmes uit.

Uploaden via beveiligde FTP

U kunt bestanden met versleuteling uploaden met behulp van FTPS in expliciete modus (FTPES) voor de verbinding met de bestemmingsbestandsserver.
Voor veilige FTP-overdracht, stelt u [Using Secure Protocol] in op [On] in de instellingen van de bestemmingsserver voor bestandsoverdracht en importeert u een certificaat.

Verwijzingen

- 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 (bevat updates per 10/06/2016).

Certificaat

Schrijf het certificaat dat wordt gebruikt door de FTPES (FTPS)-functie naar de hoofdmap van een geheugenkaart. Stel de bestandsnaam als volgt in.
certification.pem (PEM-indeling)
De maximale certificaatgrootte die kan worden geladen, is 1 MB per certificaat.

TP1002220973