MPC-2610

Bezbednosne mere predostrožnosti

Ovaj Vodič za pomoć opisuje bezbednosne mere predostrožnosti za prenos datoteka i strimovanje pomoću uređaja.

MPC-2610
Bezbednosne mere predostrožnosti

Bezbednosne mere predostrožnosti

Ova tema opisuje mere predostrožnosti prilikom povezivanja uređaja na mrežu.

- Sadržaj komunikacije može, bez vašeg znanja, da bude presretnut od strane neovlašćenih trećih lica u blizini signala. Kada koristite bežičnu LAN komunikaciju, pravilno primenite bezbednosne mere kako bi zaštitili sadržaj komunikacija.
- Ako podesite [Security] postavku za bežični LAN na [None] i povežete se na pristupnu tačku, bežična komunikacija između kamere i pristupne tačke neće biti šifrovana i može da bude presretnuta od strane trećeg lica u dometu signala. Koristite WPA2 ili WPA3 bezbednosni protokol za unapređenu bezbednost.
- KOMPANIJA SONY NEĆE BITI ODGOVORNA ZA BILO KAKVU ŠTETU NASTALU USLED NEUSPEŠNE PRIMENE ODGOVARAJUĆIH BEZBEDNOSNIH MERA NA PREDAJNICIMA, NEIZBEŽNOG CURENJA PODATAKA USLED SPECIFIKACIJA PRENOSA PODATAKA ILI BEZBEDNOSNIH PROBLEMA BILO KOJE VRSTE.
- U zavisnosti od radne okoline, neovlašćena treća lica na mreži mogu biti u mogućnosti da pristupe uređaju. Prilikom povezivanja uređaja sa mrežom, uverite se da je mreža zaštićena na odgovarajući način.
- Prilikom povezivanja ovog proizvoda na mrežu povežite se putem sistema koji poseduje funkciju zaštite, kao što je ruter ili zaštitni zid. Ako se povezivanje izvrši bez takve zaštite mogu se javiti bezbednosni problemi.

TP1002221113

MPC-2610
Bezbednosne mere predostrožnosti

Mere predostrožnosti za internet vezu

Ova tema opisuje mere predostrožnosti prilikom povezivanja uređaja na internet.

- Uređaj se ne može povezati putem bežičnog LAN-a na pristupnu tačku koja koristi samo WEP ili WPA, što su bezbednosne metode koje imaju ranjivosti.
- Uređaj nije mrežni uređaj (na primer, ruter ili prekidački hab). Izričito se preporučuje da povežete uređaj na mrežu gde možete pravilno konfigurisati i upravljati mrežnim podešavanjima kako biste se zaštitili od napada baziranih na mreži, kao što su DoS napadi (napadi uskraćivanja usluge).
- Kada povezujete uređaj na mrežu, povežite ga preko rutera koji je pravilno konfigurisan i kojim se pravilno upravlja, ili ga povežite na LAN port koji ima istu funkcionalnost. Ako je uređaj povezan bez takve zaštite (na primer, kada koristite besplatni Wi-Fi), mogu se pojaviti bezbednosni problemi. Kada su pravilno konfigurisani, ruteri pružaju dovoljnu zaštitu od DoS napada ili gubitka funkcionalnosti uređaja u mreži. Ako primetite bilo šta neobično, odmah isključite kameru iz mreže.

TP1002221114

MPC-2610
Bezbednosne mere predostrožnosti

Mere predostrožnosti u vezi sa mrežnom funkcijom

Ova tema opisuje mere predostrožnosti u vezi sa mrežnom funkcijom uređaja.

- Ako se otkrije neovlašćeni pristup, kamera može da bude onemogućena za prijem komunikacija. Ako do ovoga dođe, ponovo, iz početka, izvršite povezivanje.
- Informacije za potvrdu identiteta za povezivanje sa uređajem se prikazuju kada upotrebite [Network] – [Network Setup] – [Show Authentication]. Vodite računa da druge osobe ne vide vaš ekran i da ne mogu da kopiraju QR kod.
- Korisničko ime i lozinka moraju da se podese u trenutku kupovine. Prilikom podešavanja vašeg korisničkog imena i lozine, obratite pažnju da ove postavke ne budu vidljive drugim osobama. Korisničko ime i lozinku podesite na sledeći način.

[User Name]	– Podesite korisničko ime koje se sastoji od 1 do 16 znakova. – Fabričko podrazumevano podešavanje je „admin“. – Sledeći znakovi mogu da se unesu. Slovni znakovi (velika i mala), numerički znakovi, simboli (! % + , - . = _)
[Password]	– Podesite lozinku koja se sastoji od 8 do 16 znakova i koja sadrži najmanje 1 ili više slovnih i 1 ili više numeričkih znakova. – Sledeći znakovi mogu da se unesu. Slovni znakovi (velika i mala), numerički znakovi, simboli (! % + , - . = _)

TP1002221115

MPC-2610
Bezbednosne mere predostrožnosti

Mere predostrožnosti u vezi sa bežičnom LAN mrežom

Ova tema opisuje mere predostrožnosti prilikom povezivanja uređaja na bežičnu LAN mrežu.

- U Vodiču za pomoć ovog uređaja, pristupne tačke bežičnog LAN-a i ruteri bežičnog LAN-a koji prenose LAN vezu se nazivaju „pristupne tačke“.
- [Security] (način šifrovanja) može da se podesi na [None], [WPA2] ili [WPA3]. Upotreba [WPA2] ili [WPA3] se preporučuje sa bezbednosnog stanovišta. Kada je izabrano [None], pre povezivanja se prikazuje poruka. Za bezbednu vezu sa bežičnim LAN-om, izričito se preporučuje povezivanje sa pristupnim tačkama sa WPA2 ili WPA3 bezbednosnim podešavanjem.
- Podrazumevana postavka za bezbednosni protokol prilikom registracije pristupne tačke za bežični LAN putem [Manual Register] je WPA2.
- Ako se povežete sa pristupnom tačkom za koju nije podešena nikakva bezbednosna postavka, možete biti meta hakerskog napada, zlonamernog pristupa od strane trećih lica ili napada na ranjive tačke. Osim ukoliko to nije moguće izbeći, povezivanje bez podešenih bezbednosnih postavki se ne preporučuje.
- Konfigurisanje bezbednosnih postavki na bežičnoj LAN mreži je veoma važno. Kompanija Sony nije odgovorna za bilo kakvu štetu nastalu usled nepreduzimanja bezbednosnih mera predostrožnosti ili ukoliko dođe do bezbednosnog problema usled okolnosti pri upotrebi bežične LAN mreže koje se ne mogu izbeći.

TP1002221116

MPC-2610
Bezbednosne mere predostrožnosti

Mere predostrožnosti povezane sa USB vezivanjem

Ova tema opisuje mere predostrožnosti prilikom povezivanja jedinice preko USB vezivanja.

- Koristite samo pouzdane pametne telefone za vezivanje. Povezivanje sa uređajima nepoznatog porekla se ne preporučuje zbog bezbednosnih razloga.

TP1002221117

O FTPES (FTPS) funkciji

FTPS funkcija podržava različite algoritme za enkripciju kako bi se osigurao bezbedan prenos datoteka. Višestruki algoritmi za enkripciju, od kojih neki možda nisu u skladu sa trenutnim najboljim praksama za bezbednost, podržani su radi kompatibilnosti sa širokim spektrom servera.

Algoritmi za enkripciju koje podržava FTPS funkcija

Podržani su sledeći algoritmi za enkripciju.

- 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

Preporučeni algoritmi za enkripciju

Sledeći algoritmi za enkripciju se preporučuju na osnovu NIST preporuka (NIST SP 800-57 Deo 1 Revizija 5) i srodnih standarda bezbednosti.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

O zastarelim algoritmima

FTPS funkcija takođe podržava sledeće algoritme radi kompatibilnosti, ali su oni zastareli na osnovu NIST preporuka (NIST SP 800-57 Deo 1 Revizija 5) i srodnih standarda bezbednosti, i mogu biti uklonjeni u budućoj verziji.

- 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

O kompatibilnosti veze

FTPS funkcija je dizajnirana za ravnotežu između bezbednosti i kompatibilnosti. Trenutno su zastareli algoritmi podržani iz sledećih razloga, ali mogu biti uklonjeni u budućoj verziji kako bi se poboljšala bezbednost.

- Honorarni fotografi i video snimatelji treba da se povežu sa serverima koji rade na različitim klijentima.
- Potrebno je održavati kompatibilnost sa starijim sistemima i nasleđenim serverima.
- Nisu svi korisnici spremni da pređu na bezbednije podešavanje jer je promena podešavanja algoritama za enkripciju na serverskoj strani komplikovana.
- FTPS podešavanja se često dele sa drugim bezbednosnim uslugama. Sve promene moraju biti pažljivo razmotrene jer mogu uticati na druge usluge na serveru.
- Mora biti podržan širok spektar algoritama za enkripciju kako bi se osigurala interoperabilnost u različitim okruženjima.

Algoritam za enkripciju koji se koristi tokom FTPS veze određuje se automatskom komunikacijom sa odredišnim serverom i stoga zavisi od podešavanja servera. Iako smo svesni bezbednosnih rizika, trenutno se prioritet daje kompatibilnosti kako bi se zadovoljile raznovrsne potrebe korisnika.

Bezbednosni rizici

Korišćenje zastarelih algoritama, uključujući CBC/DHE/RSA/SHA-1, povećava rizik da šifrovani podaci mogu biti dešifrovani ili izmenjeni od strane napadača, izlažući podatke tokom prenosa.

Preporuka za bezbednu vezu

Pre korišćenja FTPS funkcije, proverite da li odredišni server za povezivanje podržava preporučeni algoritam za enkripciju. Omogućite samo preporučene algoritme na strani servera i onemogućite zastarele algoritme.

Otpremanje putem obezbeđenog FTP servera

Šifrovane datoteke možete da otpremite pomoću FTPS u eksplicitnom režimu (FTPES) za vezu sa odredišnim serverom za datoteke.
Za obezbeđeni prenos putem FTP servera, podesite [Using Secure Protocol] na [On] u podešavanjima za odredišni server za prenos podataka i uvezite sertifikat.

Reference

- 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 (uključuje ažurirane verzije od 10. 6. 2016.).

Sertifikat

Upišite sertifikat koji koristi FTPES (FTPS) funkcija u osnovni direktorijum memorijske kartice. Postavite naziv datoteke na sledeći način.
certification.pem (PEM format)
Maksimalna veličina sertifikata koja se može učitati je 1 MB po sertifikatu.

TP1002221118