ILME-FX6

Bezpečnostní opatření

Tento průvodce nápovědou popisuje bezpečnostní opatření pro přenos souborů a streamování pomocí jednotky.

ILME-FX6
Bezpečnostní opatření

Bezpečnostní opatření

Toto téma popisuje upozornění pro připojování jednotky k síti.

- Obsah komunikace může být bez vašeho vědomí odposlechnut neoprávněnými třetími stranami v blízkosti signálu. Při používání komunikace prostřednictvím bezdrátové sítě LAN zaveďte správná bezpečnostní opatřen, abyste obsah své komunikace ochránili.
- Pokud nastavíte parametry [Security] bezdrátové sítě LAN na [None] a připojíte ji k přístupovému bodu, bezdrátová komunikace mezi kamerou a přístupovým bodem nebude šifrovaná a může být zachycena třetí stranou v dosahu signálu. Pro zlepšení zabezpečení používejte bezpečnostní protokol WPA2 nebo WPA3.
- SPOLEČNOST SONY NEBUDE ODPOVĚDNÁ ZA ŠKODY ŽÁDNÉHO DRUHU, KTERÉ JSOU DŮSLEDKEM NEIMPLEMENTOVÁNÍ SPRÁVNÉHO ZABEZPEČENÍ V PŘENOSOVÝCH ZAŘÍZENÍ, NEVYHNUTELNÝCH ÚNIKŮ DAT, KTERÉ JSOU DŮSLEDKEM SPECIFIKACÍ PŘENOSOVÝCH PARAMETRŮ, NEBO PROBLÉMY ZABEZPEČENÍ JAKÉHOKOLIV DRUHU.
- V závislosti na provozních podmínkách mohou být třetí strany v síti schopny k jednotce přistupovat. Pokud jednotku připojíte do sítě, nezapomeňte si ověřit, že síť je řádně chráněna.
- V případě připojování tohoto produktu k síti se připojte pomocí systému, který poskytuje funkci ochrany, jako je například směrovač nebo brána firewall. V případě připojení bez takové ochrany se mohou vyskytnout problémy se zabezpečením.

TP1002274494

ILME-FX6
Bezpečnostní opatření

Upozornění ohledně připojení k Internetu

Toto téma popisuje upozornění pro připojování jednotky k Internetu.

- Jednotku nelze připojit prostřednictvím bezdrátové sítě LAN k přístupovému bodu, který používá pouze WEP nebo WPA, což jsou metody zabezpečení se slabými místy.
- Jednotka není síťové zařízení (např. směrovač nebo přepínací rozbočovač). Důrazně se doporučuje připojit jednotku k síti, kde můžete odpovídajícím způsobem konfigurovat a spravovat síťová nastavení s ohledem na ochranu před síťovými útoky, např. DoS (útoky zaměřené na odepření služeb).
- Při připojování jednotky k síti ji připojte prostřednictvím směrovače, který je odpovídajícím způsobem nakonfigurovaný a spravovaný, případně připojte jednotky k portu sítě LAN se stejnou funkcí. V případě připojení bez takového zabezpečení (např. při používání bezplatné Wi-Fi sítě) může dojít k bezpečnostním problémům. V případě správné konfigurace poskytují směrovače dostatečnou ochranu proti útokům DoS nebo ztrátě funkčnosti zařízení v síti. Pokud zaznamenáte cokoli neobvyklého, okamžitě odpojte kameru od sítě.

TP1002274495

Upozornění týkající se funkce sítě

Toto téma popisuje upozornění týkající se síťové funkce jednotky.

- Je-li detekován neautorizovaný přístup, kamera nemusí být schopna přijímat komunikaci. Pokud k tomu dojde, připojte znovu od začátku.
- Stisknutím tlačítka [Show Authentication] na stavové obrazovce [Network] zobrazíte informace o ověření pro připojení k jednotce. Dbejte na to, aby obrazovku nebylo možné zobrazit a aby ostatní nemohli kopírovat obraz QR kódu.
- Uživatelské jméno a heslo se generují automaticky a nastavují se v kameře v okamžiku nákupu. Při nastavování uživatelského jména a hesla dbejte na to, aby nastavení nebylo viditelné pro ostatní. Podle následujících pokynů nastavte uživatelské jméno a heslo.

[User Name]	– Nastavte uživatelské jméno o délce 1 až 16 znaků. – Výchozí tovární nastavení je „admin“. – Platné vstupní znaky jsou následující. Abecední znaky (velká a malá písmena), číselné znaky, symboly (! % + , - . = _)
[Password]	– Nastavte heslo o délce 8 až 16 znaků, které obsahuje alespoň 1 nebo více abecedních znaků a 1 nebo více číslic. – Platné vstupní znaky jsou následující. Abecední znaky (velká a malá písmena), číselné znaky, symboly (! % + , - . = _)

TP1002274496

ILME-FX6
Bezpečnostní opatření

Upozornění týkající se bezdrátové sítě LAN

Toto téma popisuje upozornění pro připojování jednotky k bezdrátové síti LAN.

- V průvodci nápovědou této jednotky jsou přístupové body bezdrátové sítě LAN a směrovače v bezdrátové síti LAN, které dokážou předávat připojení k síti LAN, označovány jako „přístupové body“.
- [Security] (metodu šifrování) lze nastavit na [None], [WPA2], nebo [WPA3]. Z bezpečnostního hlediska se doporučuje používání [WPA2] nebo [WPA3]. Když je vybrána možnost [None], před připojením se zobrazí zpráva. Pro bezpečné připojení k bezdrátové síti LAN se důrazně doporučuje připojení k přístupovým bodům s nastavením zabezpečení WPA2 nebo WPA3.
- Při registrování přístupového bodu v bezdrátové síti LAN pomocí [Manual Register] je ve výchozím nastavení vybrána metoda zabezpečení WPA2.
- Pokud se připojíte k přístupovému bodu bez nastavení zabezpečení, můžete se vystavit hacknutí, přístupu nepřátelských třetích stran a útokům na zranitelná místa. Pokud to není nevyhnutelné z jiných důvodů, připojení bez nastavení zabezpečení se nedoporučuje.
- Konfigurace zabezpečení v bezdrátové síti LAN je velmi důležitá. Společnost Sony neponese odpovědnost za jakékoli škody v důsledku nepřijetí bezpečnostních opatření ani za situaci, kdy dojde k problému s bezpečností z důvodu nevyhnutelných okolností při používání bezdrátové sítě LAN.

TP1002274497

ILME-FX6
Bezpečnostní opatření

Upozornění týkající se sdílení internetového připojení prostřednictvím USB

Toto téma popisuje upozornění pro připojování jednotky sdílením internetového připojení prostřednictvím USB.

- Pro sdílení internetového připojení USB používejte pouze důvěryhodná zařízení typu chytrého telefonu. Připojení k zařízení neznámého původu se nedoporučuje z důvodu obav o bezpečnost.

TP1002274498

ILME-FX6
Bezpečnostní opatření

O funkci FTPES (FTPS)

Funkce FTPS podporuje různé algoritmy šifrování pro zajištění bezpečného přenosu souborů. Je podporováno více algoritmů šifrování, z nichž některé nemusejí splňovat požadavky aktuálních ověřených postupů v rámci zabezpečení, z důvodu kompatibility se širokou řadou serverů.

Algoritmy šifrování podporované funkcí FTPS

Podporovány jsou následující algoritmy šifrování.

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 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

Doporučené algoritmy šifrování

Na základě doporučení NIST (NIST SP 800-57 Part 1 Revision 5) a souvisejících bezpečnostních standardů se doporučují následující algoritmy šifrování.

- 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 zastaralých algoritmech

Z důvodu kompatibility podporuje funkce FTPS i následující algoritmy, ovšem podle doporučení NIST (NIST SP 800-57 Part 1 Revision 5) a souvisejících bezpečnostních standardů jsou zastaralé a v budoucí verzi může dojít k jejich odstranění.

- 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 kompatibilitě spojení

Funkce FTPS je vytvořena s vyváženou bezpečností a kompatibilitou. Aktuálně jsou z následujících důvodů podporovány zastaralé algoritmy, ale v budoucí verzi mohou být odstraněny z důvodu zlepšení zabezpečení.

- Fotografové a kameramani na volné noze se potřebují připojovat k serverům spuštěným na různých klientech.
- Je nutno zachovat kompatibilitu se staršími systémy a servery.
- Nikoli všichni uživatelé jsou připraveni na přechod na bezpečnější nastavení, protože změna nastavení algoritmu šifrování na straně serveru je komplikovaná.
- Nastavení FTPS jsou často sdílena s jinými zabezpečenými službami. Jakékoliv změny je třeba pečlivě zvážit, protože mohou mít dopad na další služby na serveru.
- Je nutno podporovat širokou řadu algoritmů šifrování, aby byla zajištěna interoperabilita v různých prostředích.

Algoritmus šifrování používaný během připojení FTPS je určen automatickou „dohodou“ s cílovým serverem, a tak závisí na nastavení serveru. Ačkoli jsme si vědomi bezpečnostních rizik, v současnosti j upřednostňována kompatibilita, aby byly uspokojeny nejrůznější potřeby uživatelů.

Bezpečnostní rizika

Používání zastaralých algoritmů, mj. CBC/DHE/RSA/SHA-1, zvyšuje riziko, že zašifrovaná data může být možno rozšifrovat nebo zmanipulovat ze strany útočníka, a tak by data mohla být během přenosu vyzrazena.

Doporučení bezpečného spojení

Před použitím funkce FTPS ověřte, zda cílový server spojení podporuje doporučený algoritmus šifrování. Na straně serveru povolte pouze doporučené algoritmy a zakažte zastaralé algoritmy.

Odesílání pomocí zabezpečeného protokolu FTP

Soubory můžete nahrávat šifrovaně prostřednictvím protokolu FTPS v explicitním režimu (FTPES) pro připojení k cílovému souborovému serveru.
Chcete-li provést přenos protokolem Secure FTP, nastavte možnost [Using Secure Protocol] na volbu [On] na cílovém serveru přenosu souborů a importujte certifikát.

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 (včetně aktualizací ke dni 10/06/2016).

Certifikát

Zapište certifikát používaný funkcí FTPES (FTPS) do kořenového adresáře paměťové karty. Nastavte název souboru následujícím způsobem.
certification.pem (formát PEM)
Maximální velikost certifikátu, kterou lze nahrát, je 1 MB na certifikát.

TP1002274499