SFTP- / FTPES (FTPS)- / RTMPS-toiminnot

Tässä käyttöoppaassa selitetään Sony-digitaalikameroiden FTP-toiminnossa käytettävä FTP-protokolla (SFTP/FTPES (FTPS)) ja verkkosuoratoistotoiminnossa käytettävä Real-Time Messaging Protocol over SSL (RTMPS).

SFTP- / FTPES (FTPS)- / RTMPS-toiminnot

Tietoja SFTP-toiminnosta

SFTP-toiminto tukee erilaisia suojatun tiedostonsiirron salausalgoritmeja. Jotta varmistetaan yhteensopivuus erilaisten palvelimien kanssa, tuetaan useita salausalgoritmeja, myös sellaisia, jotka eivät välttämättä noudata nykyisiä suojauksen parhaita käytäntöjä.

SFTP-toiminnon tukemat salausalgoritmit

Seuraavia salausalgoritmeja tuetaan.

Key exchange algorithms

- curve25519-sha256
- curve25519-sha256@libssh.org
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group-exchange-sha1

Host key algorithms

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- ssh-ed25519
- ssh-rsa
- ssh-dss

Ciphers

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes256-cbc
- rijndael-cbc@lysator.liu.se
- aes192-cbc
- aes128-cbc
- blowfish-cbc
- arcfour128
- arcfour
- cast128-cbc
- 3des-cbc

MACs

- hmac-sha2-256

- hmac-sha2-512
- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- hmac-ripemd160@openssh.com

Tietoja suositeltavista salausalgoritmeista

NIST-suositusten (NIST SP 800-57 Part 1, Revision 5) ja niihin liittyvien turvallisuusstandardien perusteella suositellaan seuraavia salausalgoritmeja.

Key exchange algorithms

- curve25519-sha256
- curve25519-sha256@libssh.org
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512

Host key algorithms

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- ssh-ed25519

Ciphers

- aes128-ctr
- aes192-ctr
- aes256-ctr

MACs

- hmac-sha2-256
- hmac-sha2-512

Tietoja vanhentuneista algoritmeista

SFTP-toiminto tukee myös seuraavia algoritmeja yhteensopivuussyistä, mutta ne ovat vanhentuneita NIST-suositusten (NIST SP 800-57 Part 1, Revision 5) ja niihin liittyvien turvallisuusstandardien perusteella, ja ne saatetaan poistaa tulevista versioista.

Key exchange algorithms

- diffie-hellman-group14-sha256
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group-exchange-sha1

Host key algorithms

- ssh-dss
- ssh-rsa

Ciphers

- rijndael-cbc@lysator.liu.se
- blowfish-cbc
- arcfour128
- arcfour
- cast128-cbc
- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc

MACs

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- hmac-ripemd160@openssh.com

Yhteyden yhteensopivuus

SFTP-toiminto on suunniteltu tasapainottamaan turvallisuus ja yhteensopivuus. Vanhentuneita algoritmeja tuetaan tällä hetkellä seuraavista syistä, mutta nämä algoritmit voidaan poistaa tulevista versioista turvallisuuden parantamiseksi.

- Freelance-valokuvaajien ja -videokuvaajien täytyy muodostaa yhteys eri asiakkaiden ylläpitämiin palvelimiin.
- Yhteensopivuus vanhempien järjestelmien ja vanhojen palvelimien kanssa täytyy säilyttää.
- Salausalgoritmin asetusten muuttaminen palvelimen puolella on monimutkaista, eivätkä kaikki käyttäjät ole valmiita vaihtamaan suojattuun asetukseen.
- SFTP-palvelinasetukset jaetaan usein muiden turvallisten palveluiden kanssa, joten on otettava huomioon vaikutukset muihin palveluihin palvelimella, eikä muutosten toteuttaminen välttämättä ole aina helppoa.
- Yhteentoimivuuden varmistamiseksi eri ympäristöissä tarvitaan tukea monenlaisille salausalgoritmeille.

SFTP-yhteyden aikana käytettävä salausalgoritmi määritetään automaattisella neuvottelulla kohdepalvelimen kanssa, joten se riippuu palvelimen asetuksista. Vaikka olemme tietoisia turvallisuusriskeistä, asetamme tällä hetkellä laajan yhteensopivuuden etusijalle vastataksemme käyttäjien erilaisiin tarpeisiin.

Turvallisuusriskit

Vanhentuneiden algoritmien käyttö lisää SHA-1-pohjaisten algoritmien ja DSA-avainten haavoittuvuutta väliintulohyökkäyksille, palvelimen tunnistetietojen väärentämisriskille ja kryptoanalyysin mahdollisuudelle vanhempien salausalgoritmien kanssa (esim. 3DES- ja RC4-variantit), jotka voivat paljastaa tietoja siirron aikana.

Turvallista yhteyttä koskevat suositukset

Tarkista SFTP-asiakastoimintoa käytettäessä etukäteen, tukeeko palvelin, johon yhteys muodostetaan, suositeltuja salausalgoritmeja. On suositeltavaa ottaa käyttöön vain suositellut algoritmit ja poistaa ei-suositellut algoritmit käytöstä palvelimen puolella.

Lähteet

- 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 (includes updates as of 10/06/2016).

SFTP- / FTPES (FTPS)- / RTMPS-toiminnot

Tietoja FTPES (FTPS) -toiminnosta

FTPES (FTPS) -toiminto tukee erilaisia suojatun tiedostonsiirron salausalgoritmeja. Jotta varmistetaan yhteensopivuus erilaisten palvelimien kanssa, tuetaan useita salausalgoritmeja, myös sellaisia, jotka eivät välttämättä noudata nykyisiä suojauksen parhaita käytäntöjä.

FTPES (FTPS) -toiminnon tukemat salausalgoritmit

Seuraavia salausalgoritmeja tuetaan.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Tietoja suositeltavista salausalgoritmeista

NIST-suositusten (NIST SP 800-57 Part 1, Revision 5) ja niihin liittyvien turvallisuusstandardien perusteella suositellaan seuraavia salausalgoritmeja.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Tietoja vanhentuneista algoritmeista

FTPES (FTPS) -toiminto tukee myös seuraavia algoritmeja yhteensopivuussyistä, mutta ne ovat vanhentuneita NIST-suositusten (NIST SP 800-57 Part 1, Revision 5) ja niihin liittyvien turvallisuusstandardien perusteella, ja ne saatetaan poistaa tulevista versioista.

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Yhteyden yhteensopivuus

FTPES (FTPS) -toiminto on suunniteltu tasapainottamaan turvallisuus ja yhteensopivuus. Vanhentuneita algoritmeja tuetaan tällä hetkellä seuraavista syistä, mutta nämä algoritmit voidaan poistaa tulevista versioista turvallisuuden parantamiseksi.

- Freelance-valokuvaajien ja -videokuvaajien täytyy muodostaa yhteys eri asiakkaiden ylläpitämiin palvelimiin.
- Yhteensopivuus vanhempien järjestelmien ja vanhojen palvelimien kanssa täytyy säilyttää.
- Salausalgoritmin asetusten muuttaminen palvelimen puolella on monimutkaista, eivätkä kaikki käyttäjät ole valmiita vaihtamaan suojattuun asetukseen.
- FTPES (FTPS) -palvelinasetukset jaetaan usein muiden turvallisten palveluiden kanssa, joten on otettava huomioon vaikutukset muihin palveluihin palvelimella, eikä muutosten toteuttaminen välttämättä ole aina helppoa.
- Yhteentoimivuuden varmistamiseksi eri ympäristöissä tarvitaan tukea monenlaisille salausalgoritmeille.

FTPES (FTPS) -yhteyden aikana käytettävä salausalgoritmi määritetään automaattisella neuvottelulla kohdepalvelimen kanssa, joten se riippuu palvelimen asetuksista. Vaikka olemme tietoisia turvallisuusriskeistä, asetamme tällä hetkellä laajan yhteensopivuuden etusijalle vastataksemme käyttäjien erilaisiin tarpeisiin.

Turvallisuusriskit

Vanhentuneiden algoritmien, mukaan lukien CBC/DHE/RSA/SHA-1, käyttäminen lisää riskiä, että hyökkääjä voi purkaa salatun datan tai peukaloida sitä, jolloin tiedot paljastuvat siirron aikana.

Turvallista yhteyttä koskevat suositukset

Tarkista FTPES (FTPS) -asiakastoimintoa käytettäessä etukäteen, tukeeko palvelin, johon yhteys muodostetaan, suositeltuja salausalgoritmeja. On suositeltavaa ottaa käyttöön vain suositellut algoritmit ja poistaa ei-suositellut algoritmit käytöstä palvelimen puolella.

Lähteet

- 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 (includes updates as of 10/06/2016).

TP1002071182

SFTP- / FTPES (FTPS)- / RTMPS-toiminnot

Tietoja RTMPS-toiminnosta

RTMPS-toiminto tukee erilaisia salausalgoritmeja suojattua RTMPS-suoratoistoa varten. Jotta varmistetaan yhteensopivuus erilaisten kohdepalvelimien kanssa, tuetaan useita salausalgoritmeja, myös sellaisia, jotka eivät välttämättä noudata nykyisiä suojauksen parhaita käytäntöjä.

RTMPS-toiminnon tukemat salausalgoritmit

Seuraavia salausalgoritmeja tuetaan.

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Tietoja suositeltavista salausalgoritmeista

NIST-suositusten (NIST SP 800-57 Part 1, Revision 5) ja niihin liittyvien turvallisuusstandardien perusteella suositellaan seuraavia salausalgoritmeja.

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Tietoja vanhentuneista algoritmeista

RTMPS-toiminto tukee myös seuraavia algoritmeja yhteensopivuussyistä, mutta ne ovat vanhentuneita NIST-suositusten (NIST SP 800-57 Part 1, Revision 5) ja niihin liittyvien turvallisuusstandardien perusteella, ja ne saatetaan poistaa tulevista versioista.

Key exchange algorithms

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Yhteyden yhteensopivuus

RTMPS-toiminto on suunniteltu tasapainottamaan turvallisuus ja yhteensopivuus. Vanhentuneita algoritmeja tuetaan tällä hetkellä seuraavista syistä, mutta nämä algoritmit voidaan poistaa tulevista versioista turvallisuuden parantamiseksi.

- RTMPS-suoratoistotoiminnon käyttämistä varten täytyy muodostaa yhteys erilaisiin palvelimiin, jotka tukevat RTMPS-toimitusta.
- Yhteensopivuus vanhempien järjestelmien ja vanhojen palvelimien kanssa täytyy säilyttää.
- Salausalgoritmin asetusten muuttaminen palvelimen puolella on monimutkaista, eivätkä kaikki käyttäjät ole valmiita vaihtamaan suojattuun asetukseen.
- RTMPS-palvelinasetukset jaetaan usein muiden turvallisten palveluiden kanssa, joten on otettava huomioon vaikutukset muihin palveluihin palvelimella, eikä muutosten toteuttaminen välttämättä ole aina helppoa.
- Yhteentoimivuuden varmistamiseksi eri ympäristöissä tarvitaan tukea monenlaisille salausalgoritmeille.

RTMPS-yhteyden aikana käytettävä salausalgoritmi määritetään automaattisella neuvottelulla kohdepalvelimen kanssa, joten se riippuu palvelimen asetuksista. Vaikka olemme tietoisia turvallisuusriskeistä, asetamme tällä hetkellä laajan yhteensopivuuden etusijalle vastataksemme käyttäjien erilaisiin tarpeisiin.

Turvallisuusriskit

Vanhentuneiden algoritmien, mukaan lukien CBC ja DHE, käyttäminen lisää riskiä, että hyökkääjä voi purkaa salatun datan, jolloin tiedot paljastuvat suoratoiston aikana.

Turvallista yhteyttä koskevat suositukset

Tarkista RTMPS-suoratoistotoimintoa käytettäessä etukäteen, tukeeko palvelin, johon yhteys muodostetaan, suositeltuja salausalgoritmeja. On suositeltavaa ottaa käyttöön vain suositellut algoritmit ja poistaa ei-suositellut algoritmit käytöstä palvelimen puolella.

Lähteet

- 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 (includes updates as of 10/06/2016).

TP1002071183