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

Denne hjelpeveiledningen forklarer filoverføringsprotokollen (SFTP / FTPES (FTPS)) som brukes i FTP-funksjonen, og meldingsprotokollen i sanntid over SSL (RTMPS) som brukes i nettverksstrømmingsfunksjonen på Sony digitalkameraer.

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

Om SFTP-funksjonen

SFTP-funksjonen støtter en rekke krypteringsalgoritmer for sikre filoverføringer. For å sikre kompatibilitet med en lang rekke servere, støttes flere krypteringsalgoritmer, inkludert noen som kanskje ikke er i samsvar med den beste sikkerheten.

Krypteringsalgoritmer som støttes av SFTP-funksjonen

Følgende krypteringsalgoritmer støttes.

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

Om anbefalte krypteringsalgoritmer

Basert på NIST-anbefalingene (NIST SP 800-57 Part 1, Revision 5) og relaterte sikkerhetsstandarder, anbefales følgende krypteringsalgoritmer:

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

Om foreldede algoritmer

SFTP-funksjonen støtter også følgende algoritmer av kompatibilitetsgrunner, men de er foreldet i henhold til NIST-anbefalingene (NIST SP 800-57 Part 1, Revision 5) og relaterte sikkerhetsstandarder, og kan bli fjernet i fremtidige versjoner.

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

Kompatibilitet med tilkobling

SFTP-funksjonen er utformet for å balansere sikkerhet og kompatibilitet. For øyeblikket støtter vi foreldede algoritmer av følgende årsaker, men vi kan fjerne disse algoritmene i fremtidige versjoner for å forbedre sikkerheten.

- Frilansfotografer og videografer må koble til servere som driftes av ulike klienter.
- Kompatibilitet med eldre systemer og gamle servere må opprettholdes.
- Det er komplekst å endre innstillingene for krypteringsalgoritmer på serversiden, og ikke alle brukere er forberedt på å endre til en sikker innstilling.
- SFTP-serverinnstillinger deles ofte med andre sikre tjenester, så det er nødvendig å vurdere virkningen på andre tjenester på serveren, og det kan hende at det ikke alltid er lett å implementere endringer.
- For å sikre interoperabilitet i ulike miljøer er det nødvendig med støtte for et bredt spekter av kryptografiske algoritmer.

Krypteringsalgoritmen som benyttes under SFTP-tilkoblingen, bestemmes av automatisk forhandling med målserveren, så det avhenger av serverens innstillinger. Vi er oppmerksomme på sikkerhetsrisikoene, men prioriterer for øyeblikket bred kompatibilitet for å møte de forskjellige behovene til brukerne våre.

Sikkerhetsrisikoer

Bruk av foreldede algoritmer øker sårbarheten til SHA-1-baserte algoritmer og DSA-nøkler for MitM-angrep, risiko for falsk serveridentitet og mulighet for kryptoanalyse med eldre krypteringsalgoritmer (f.eks. 3DES- og RC4-varianter), noe som kan eksponere data under overføring.

Anbefalinger for en sikker tilkobling

Når du bruker SFTP-klientfunksjonen, må du på forhånd kontrollere om serveren du kobler til, støtter de anbefalte krypteringsalgoritmene. Vi anbefaler at du bare aktiverer anbefalte algoritmer, og deaktiverer ikke-anbefalte algoritmer på serversiden.

Referanser

- 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-funksjonene

Om FTPES-funksjonen (FTPS)

FTPES-funksjonen (FTPS) støtter en rekke krypteringsalgoritmer for sikre filoverføringer. For å sikre kompatibilitet med en lang rekke servere, støttes flere krypteringsalgoritmer, inkludert noen som kanskje ikke er i samsvar med den beste sikkerheten.

Krypteringsalgoritmer som støttes av FTPES-funksjonen (FTPS)

Følgende krypteringsalgoritmer støttes.

- 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

Om anbefalte krypteringsalgoritmer

Basert på NIST-anbefalingene (NIST SP 800-57 Part 1, Revision 5) og relaterte sikkerhetsstandarder, anbefales følgende krypteringsalgoritmer:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Om foreldede algoritmer

FTPES-funksjonen (FTPS) støtter også følgende algoritmer av kompatibilitetsgrunner, men de er foreldet i henhold til NIST-anbefalingene (NIST SP 800-57 Part 1, Revision 5) og relaterte sikkerhetsstandarder, og kan bli fjernet i fremtidige versjoner.

- 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

Kompatibilitet med tilkobling

FTPES-funksjonen (FTPS) er utformet for å balansere sikkerhet og kompatibilitet. For øyeblikket støtter vi foreldede algoritmer av følgende årsaker, men vi kan fjerne disse algoritmene i fremtidige versjoner for å forbedre sikkerheten.

- Frilansfotografer og videografer må koble til servere som driftes av ulike klienter.
- Kompatibilitet med eldre systemer og gamle servere må opprettholdes.
- Det er komplekst å endre innstillingene for krypteringsalgoritmer på serversiden, og ikke alle brukere er forberedt på å endre til en sikker innstilling.
- FTPES-serverinnstillingene (FTPS) deles ofte med andre sikre tjenester, så det er nødvendig å vurdere virkningen på andre tjenester på serveren, og det kan hende at det ikke alltid er lett å implementere endringer.
- For å sikre interoperabilitet i ulike miljøer, er det nødvendig med støtte for et bredt spekter av kryptografiske algoritmer.

Krypteringsalgoritmen som benyttes under FTPES-tilkoblingen (FTPS), bestemmes av automatisk forhandling med målserveren, så det avhenger av serverens innstillinger. Vi er oppmerksomme på sikkerhetsrisikoene, men prioriterer for øyeblikket bred kompatibilitet for å møte de forskjellige behovene til brukerne våre.

Sikkerhetsrisikoer

Bruk av foreldede algoritmer, inkludert CBC/DHE/RSA/SHA-1, øker risikoen for at krypterte data kan dekrypteres eller tukles med av en angriper, noe som eksponerer data under overføring.

Anbefalinger for en sikker tilkobling

Når du bruker FTPES-klientfunksjonen (FTPS), må du på forhånd kontrollere om serveren du kobler til, støtter de anbefalte krypteringsalgoritmene. Vi anbefaler at du bare aktiverer anbefalte algoritmer, og deaktiverer ikke-anbefalte algoritmer på serversiden.

Referanser

- 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).

TP1002071187

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

Om RTMPS-funksjonen

RTMPS-funksjonen støtter en rekke krypteringsalgoritmer for sikker RTMPS-strømming. For å sikre kompatibilitet med en lang rekke målservere, støttes flere krypteringsalgoritmer, inkludert noen som kanskje ikke er i samsvar med den beste sikkerheten.

Krypteringsalgoritmer som støttes av RTMPS-funksjonen

Følgende krypteringsalgoritmer støttes:

- 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

Om anbefalte krypteringsalgoritmer

Basert på NIST-anbefalingene (NIST SP 800-57 Part 1, Revision 5) og relaterte sikkerhetsstandarder, anbefales følgende krypteringsalgoritmer:

- 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

Om foreldede algoritmer

RTMPS-funksjonen støtter også følgende algoritmer av kompatibilitetsgrunner, men de er foreldet i henhold til NIST-anbefalingene (NIST SP 800-57 Part 1, Revision 5) og relaterte sikkerhetsstandarder, og kan bli fjernet i fremtidige versjoner.

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

Kompatibilitet med tilkobling

RTMPS-funksjonen er utformet for å balansere sikkerhet og kompatibilitet. For øyeblikket støtter vi foreldede algoritmer av følgende årsaker, men vi kan fjerne disse algoritmene i fremtidige versjoner for å forbedre sikkerheten.

- For å bruke RTMPS-strømmingsfunksjonen må du koble til ulike servere som støtter RTMPS-levering.
- Kompatibilitet med eldre systemer og gamle servere må opprettholdes.
- Det er komplekst å endre innstillingene for krypteringsalgoritmer på serversiden, og ikke alle brukere er forberedt på å endre til en sikker innstilling.
- RTMPS-serverinnstillinger deles ofte med andre sikre tjenester, så det er nødvendig å vurdere virkningen på andre tjenester på serveren, og det kan hende at det ikke alltid er lett å implementere endringer.
- For å sikre interoperabilitet i ulike miljøer, er det nødvendig med støtte for et bredt spekter av kryptografiske algoritmer.

Krypteringsalgoritmen som benyttes under RTMPS-tilkoblingen, bestemmes av automatisk forhandling med målserveren, så det avhenger av serverens innstillinger. Vi er oppmerksomme på sikkerhetsrisikoene, men prioriterer for øyeblikket bred kompatibilitet for å møte de forskjellige behovene til brukerne våre.

Sikkerhetsrisikoer

Bruk av foreldede algoritmer, inkludert CBC og DHE, øker risikoen for at krypterte data kan dekrypteres av en angriper, noe som eksponerer dataene som strømmes.

Anbefalinger for en sikker tilkobling

Når du bruker RTMPS-strømmingsfunksjonen, må du på forhånd kontrollere om serveren du kobler til, støtter de anbefalte krypteringsalgoritmene. Vi anbefaler at du bare aktiverer anbefalte algoritmer, og deaktiverer ikke-anbefalte algoritmer på serversiden.

Referanser

- 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).

TP1002071188