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

I denna hjälpguide förklaras File Transfer Protocol (SFTP/FTPES (FTPS)) som används i funktionen FTP och Real-Time Messaging Protocol över SSL (RTMPS) som används i funktionen för nätverksströmning i digitalkameror från Sony.

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

Angående SFTP-funktionen

SFTP-funktionen stöder en rad olika krypteringsalgoritmer för säkra filöverföringar. För att säkerställa kompatibilitet med ett stort antal servrar stöds flera krypteringsalgoritmer, inklusive vissa som inte följer gällande säkerhetsmetoder.

Krypteringsalgoritmer som stöds av SFTP-funktionen

Följande krypteringsalgoritmer stöds.

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

Angående rekommenderade krypteringsalgoritmer

Baserat på NIST-rekommendationer (NIST SP 800-57 Part 1, Revision 5) och relaterade säkerhetsstandarder rekommenderas följande 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

Angående föråldrade algoritmer

SFTP-funktionen stöder även följande algoritmer av kompatibilitetsskäl men de är föråldrade baserat på NIST-rekommendationerna (NIST SP 800-57 Part 1, Revision 5) och relaterade säkerhetsstandarder och kan tas bort i framtida versioner.

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

Anslutningskompatibilitet

SFTP-funktionen är utformad för att balansera säkerhet och kompatibilitet. För närvarande har vi stöd för föråldrade algoritmer av följande orsaker men vi kan ta bort dessa algoritmer i framtida versioner för att öka säkerheten.

- Frilansande fotografer och videoinspelare måste ansluta till servrar som drivs av olika klienter.
- Kompatibilitet med äldre system och gamla servrar måste upprätthållas.
- Att ändra inställningarna för krypteringsalgoritmer på serversidan är komplicerat och inte alla användare är redo att ändra till en säker inställning.
- SFTP-serverinställningar delas ofta med andra säkra tjänster, så det är nödvändigt att beakta inverkan på andra tjänster på servern och ändringar är kanske inte alltid lätta att genomföra.
- För att säkerställa interoperabilitet i olika miljöer krävs stöd för en mängd kryptografiska algoritmer.

Krypteringsalgoritmen som används under SFTP-anslutning bestäms av automatisk förhandling med målservern, vilket beror på serverns inställningar. Vi är medvetna om säkerhetsriskerna och vi prioriterar för närvarande bred kompatibilitet för att uppfylla våra användares olika behov.

Säkerhetsrisker

Användningen av föråldrade algoritmer ökar sårbarheten för SHA-1-baserade algoritmer och DSA-nycklar för man-in-the-middle-attacker, risken för kapning av serverns identitet samt möjligheten att kryptoanalys fungerar med äldre krypterade algoritmer (t.ex. 3DES- och RC4-varianter) som kan exponera data som överförs.

Rekommendationer för en säker anslutning

Om du använder SFTP-klientfunktionen ska du kontrollera i förväg om servern som du ansluter till har stöd för de rekommenderade krypteringsalgoritmerna. Vi rekommenderar att du bara aktiverar de rekommenderade algoritmerna och avaktiverar icke-rekommenderade algoritmer på serversidan.

Referenser

- 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-funktionerna

Angående FTPES (FTPS)-funktionen

FTPES-funktionen (FTPS) stöder en rad olika krypteringsalgoritmer för säkra filöverföringar. För att säkerställa kompatibilitet med ett stort antal servrar stöds flera krypteringsalgoritmer, inklusive vissa som inte följer gällande säkerhetsmetoder.

Krypteringsalgoritmer som stöds av FTPES-funktionen (FTPS)

Följande krypteringsalgoritmer stöds.

- 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

Angående rekommenderade krypteringsalgoritmer

Baserat på NIST-rekommendationer (NIST SP 800-57 Part 1, Revision 5) och relaterade säkerhetsstandarder rekommenderas följande 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

Angående föråldrade algoritmer

FTPES-funktionen (FTPS) stöder även följande algoritmer av kompatibilitetsskäl men de är föråldrade baserat på NIST-rekommendationerna (NIST SP 800-57 Part 1, Revision 5) och relaterade säkerhetsstandarder och kan tas bort i framtida versioner.

- 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

Anslutningskompatibilitet

FTPES-funktionen (FTPS) är utformad för att balansera säkerhet och kompatibilitet. För närvarande har vi stöd för föråldrade algoritmer av följande orsaker men vi kan ta bort dessa algoritmer i framtida versioner för att öka säkerheten.

- Frilansande fotografer och videoinspelare måste ansluta till servrar som drivs av olika klienter.
- Kompatibilitet med äldre system och gamla servrar måste upprätthållas.
- Att ändra inställningarna för krypteringsalgoritmer på serversidan är komplicerat och inte alla användare är redo att ändra till en säker inställning.
- FTPES (FTPS)-serverinställningar delas ofta med andra säkra tjänster, så det är nödvändigt att beakta inverkan på andra tjänster på servern och ändringar är kanske inte alltid lätta att genomföra.
- För att säkerställa interoperabilitet i olika miljöer krävs stöd för en mängd kryptografiska algoritmer.

Krypteringsalgoritmen som används under FTPES (FTPS)-anslutning bestäms av automatisk förhandling med målservern, vilket beror på serverns inställningar. Vi är medvetna om säkerhetsriskerna och vi prioriterar för närvarande bred kompatibilitet för att uppfylla våra användares olika behov.

Säkerhetsrisker

Användningen av föråldrade algoritmer, inklusive CBC/DHE/RSA/SHA-1 ökar risken att krypterade data dekrypteras eller manipuleras av en angripare, vilket exponerar data som överförs.

Rekommendationer för en säker anslutning

När du använder FTPES (FTPS)-klientfunktionen ska du kontrollera i förväg om servern som du ansluter till har stöd för de rekommenderade krypteringsalgoritmerna. Vi rekommenderar att du bara aktiverar de rekommenderade algoritmerna och avaktiverar icke-rekommenderade algoritmer på serversidan.

Referenser

- 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).

TP1002071177

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

Angående RTMPS-funktionen

RTMPS-funktionen stöder en rad olika krypteringsalgoritmer för säker RTMPS-strömning. För att säkerställa kompatibilitet med ett stort antal målservrar stöds flera krypteringsalgoritmer, inklusive vissa som inte följer gällande säkerhetsmetoder.

Krypteringsalgoritmer som stöds av RTMPS-funktionen

Följande krypteringsalgoritmer stöds.

- 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

Angående rekommenderade krypteringsalgoritmer

Baserat på NIST-rekommendationer (NIST SP 800-57 Part 1, Revision 5) och relaterade säkerhetsstandarder rekommenderas följande 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

Angående föråldrade algoritmer

RTMPS-funktionen stöder även följande algoritmer av kompatibilitetsskäl men de är föråldrade baserat på NIST-rekommendationerna (NIST SP 800-57 Part 1, Revision 5) och relaterade säkerhetsstandarder och kan tas bort i framtida versioner.

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

Anslutningskompatibilitet

RTMPS-funktionen är utformad för att balansera säkerhet och kompatibilitet. För närvarande har vi stöd för föråldrade algoritmer av följande orsaker men vi kan ta bort dessa algoritmer i framtida versioner för att öka säkerheten.

- För att använda RTMPS-strömningsfunktionen måste du ansluta till olika servrar med stöd för RTMPS-leverans.
- Kompatibilitet med äldre system och gamla servrar måste upprätthållas.
- Att ändra inställningarna för krypteringsalgoritmer på serversidan är komplicerat och inte alla användare är redo att ändra till en säker inställning.
- RTMPS-serverinställningar delas ofta med andra säkra tjänster, så det är nödvändigt att beakta inverkan på andra tjänster på servern och ändringar är kanske inte alltid lätta att genomföra.
- För att säkerställa interoperabilitet i olika miljöer krävs stöd för en mängd kryptografiska algoritmer.

Krypteringsalgoritmen som används under RTMPS-anslutning bestäms av automatisk förhandling med målservern, vilket beror på serverns inställningar. Vi är medvetna om säkerhetsriskerna och vi prioriterar för närvarande bred kompatibilitet för att uppfylla våra användares olika behov.

Säkerhetsrisker

Användningen av föråldrade algoritmer, inklusive CBC och DHE ökar risken att krypterade data dekrypteras eller manipuleras av en angripare, vilket exponerar data som strömmas.

Rekommendationer för en säker anslutning

Om du använder RTMPS-strömningsfunktionen ska du kontrollera i förväg om servern som du ansluter till har stöd för de rekommenderade krypteringsalgoritmerna. Vi rekommenderar att du bara aktiverar de rekommenderade algoritmerna och avaktiverar icke-rekommenderade algoritmer på serversidan.

Referenser

- 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).

TP1002071178