De functies SFTP, FTPES (FTPS) en RTMPS

Deze Helpgids beschrijft het File Transfer Protocol (bestandsoverdrachtprotocol, SFTP / FTPES (FTPS)) dat wordt gebruikt in de FTP-functie, en het Real-Time Messaging Protocol over SSL (realtime berichtenprotocol via SSL, RTMPS) dat wordt gebruikt in de netwerkstreamingfunctie van de digitale camera's van Sony.

Over de SFTP-functie

Over de FTPES (FTPS)-functie

Over de RTMPS-functie

De functies SFTP, FTPES (FTPS) en RTMPS

Over de SFTP-functie

De SFTP-functie ondersteunt een groot aantal versleutelingsalgoritmen voor een veilige bestandsoverdracht. Om compatibiliteit met een breed scala aan servers te garanderen, worden diverse versleutelingsalgoritmen ondersteund, waaronder sommige die niet voldoen aan de huidige, beste beveiligingsmethoden.

Versleutelingsalgoritmen die door de SFTP-functie worden ondersteund

De volgende versleutelingsalgoritmen worden ondersteund.

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

Over aanbevolen versleutelingsalgoritmen

Op basis van de NIST-aanbevelingen (NIST SP 800-57 Part 1, Revision 5) en gerelateerde beveiligingsnormen, worden de volgende versleutelingsalgoritmen aanbevolen.

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

Over verouderde algoritmen

De SFTP-functie ondersteunt tevens de volgende algoritmen omwille van de compatibiliteit, maar deze zijn verouderd op basis van de NIST-aanbevelingen (NIST SP 800-57 Part 1, Revision 5) en gerelateerde beveiligingsnormen, en kunnen in toekomstige versies worden verwijderd.

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

Compatibiliteit van de verbinding

De SFTP-functie is ontworpen om beveiliging en compatibiliteit in evenwicht te brengen. Momenteel ondersteunen we verouderde algoritmen om de volgende redenen, maar we kunnen deze algoritmen in toekomstige versies verwijderen om de beveiliging te verbeteren.

- Freelance fotografen en videografen moeten verbinding kunnen maken met servers die door diverse clients worden gebruikt.
- Compatibiliteit met oudere systemen en legacy-servers moet worden behouden.
- Het wijzigen van de instellingen voor het versleutelingsalgoritme aan de server-kant is complex en niet alle gebruikers zijn bereid om te veranderen naar een veilige instelling.
- SFTP-serverinstellingen worden vaak gedeeld met andere beveiligde services, dus is het noodzakelijk om rekening te houden met de gevolgen voor andere services op de server, en dat wijzigingen niet altijd eenvoudig zijn te implementeren.
- Om de interoperabiliteit in verschillende omgevingen te garanderen, is het noodzakelijk om een breed scala aan cryptografische algoritmen te ondersteunen.

Het versleutelingsalgoritme dat tijdens de SFTP-verbinding wordt gebruikt, wordt bepaald tijdens automatische onderhandeling met de bestemmingsserver, en is dus afhankelijk van de instellingen op de server. Ondanks dat wij ons bewust zijn van de veiligheidsrisico's, geven we momenteel de voorkeur aan een brede compatibiliteit om tegemoet te komen aan de diverse behoeften van onze gebruikers.

Beveiligingsrisico's

Het gebruik van verouderde algoritmen verhoogt de kwetsbaarheid van algoritmen gebaseerd op SHA-1 en van DSA-sleutels voor 'man-in-the-middle'-aanvallen, het risico van serveridentiteit-spoofing en de mogelijkheid van versleutelingsanalyse met oudere versleutelingsalgoritmen (bijvoorbeeld 3DES- en RC4-varianten) waardoor de gegevens tijdens de overdracht kunnen worden onderschept.

Aanbevelingen voor een beveiligde verbinding

Als u de SFTP-clientfunctie gebruikt, controleert u van tevoren of de server waarmee u verbinding maakt, de aanbevolen versleutelingsalgoritmen ondersteunt. Wij adviseren u alleen de aanbevolen algoritmen inschakelt en alle niet-aanbevolen algoritmen uitschakelt aan de server-kant.

Verwijzingen

- 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).

TP1002071126

De functies SFTP, FTPES (FTPS) en RTMPS

Over de FTPES (FTPS)-functie

De FTPES (FTPS)-functie ondersteunt een groot aantal versleutelingsalgoritmen voor een veilige bestandsoverdracht. Om compatibiliteit met een breed scala aan servers te garanderen, worden diverse versleutelingsalgoritmen ondersteund, waaronder sommige die niet voldoen aan de huidige, beste beveiligingsmethoden.

Versleutelingsalgoritmen die door de FTPES (FTPS)-functie worden ondersteund

De volgende versleutelingsalgoritmen worden ondersteund.

- 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

Over aanbevolen versleutelingsalgoritmen

Op basis van de NIST-aanbevelingen (NIST SP 800-57 Part 1, Revision 5) en gerelateerde beveiligingsnormen, worden de volgende versleutelingsalgoritmen aanbevolen.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Over verouderde algoritmen

De FTPES (FTPS)-functie ondersteunt tevens de volgende algoritmen omwille van de compatibiliteit, maar deze zijn verouderd op basis van de NIST-aanbevelingen (NIST SP 800-57 Part 1, Revision 5) en gerelateerde beveiligingsnormen, en kunnen in toekomstige versies worden verwijderd.

- 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

Compatibiliteit van de verbinding

De FTPES (FTPS)-functie is ontworpen om de beveiliging en compatibiliteit in evenwicht te brengen. Momenteel ondersteunen we verouderde algoritmen om de volgende redenen, maar we kunnen deze algoritmen in toekomstige versies verwijderen om de beveiliging te verbeteren.

- Freelance fotografen en videografen moeten verbinding kunnen maken met servers die door diverse clients worden gebruikt.
- Compatibiliteit met oudere systemen en legacy-servers moet worden behouden.
- Het wijzigen van de instellingen voor het versleutelingsalgoritme aan de server-kant is complex en niet alle gebruikers zijn bereid om te veranderen naar een veilige instelling.
- FTPES (FTPS)-serverinstellingen worden vaak gedeeld met andere beveiligde services, dus is het noodzakelijk om rekening te houden met de gevolgen voor andere services op de server, en dat wijzigingen niet altijd eenvoudig zijn te implementeren.
- Om de interoperabiliteit in verschillende omgevingen te garanderen, is het noodzakelijk om een breed scala aan cryptografische algoritmen te ondersteunen.

Het versleutelingsalgoritme dat tijdens de FTPES (FTPS)-verbinding wordt gebruikt, wordt bepaald tijdens automatische onderhandeling met de bestemmingsserver, en is dus afhankelijk van de instellingen op de server. Ondanks dat wij ons bewust zijn van de veiligheidsrisico's, geven we momenteel de voorkeur aan een brede compatibiliteit om tegemoet te komen aan de diverse behoeften van onze gebruikers.

Beveiligingsrisico's

Het gebruik van verouderde algoritmen, waaronder CBC, DHE, RSA en SHA-1, verhoogt het risico dat versleutelde gegevens worden ontsleuteld of gemanipuleerd door een aanvaller, waardoor de gegevens tijdens de overdracht kunnen worden onderschept.

Aanbevelingen voor een beveiligde verbinding

Als u de FTPES (FTPS)-clientfunctie gebruikt, controleert u van tevoren of de server waarmee u verbinding maakt, de aanbevolen versleutelingsalgoritmen ondersteunt. Wij adviseren u alleen de aanbevolen algoritmen inschakelt en alle niet-aanbevolen algoritmen uitschakelt aan de server-kant.

Verwijzingen

- 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).

TP1002071127

De functies SFTP, FTPES (FTPS) en RTMPS

Over de RTMPS-functie

De RTMPS-functie ondersteunt een groot aantal versleutelingsalgoritmen voor beveiligde RTMPS-streaming. Om compatibiliteit met een breed scala aan bestemmingsservers te garanderen, worden diverse versleutelingsalgoritmen ondersteund, waaronder sommige die niet voldoen aan de huidige, beste beveiligingsmethoden.

Versleutelingsalgoritmen die door de RTMPS-functie worden ondersteund

De volgende versleutelingsalgoritmen worden ondersteund.

- 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

Over aanbevolen versleutelingsalgoritmen

Op basis van de NIST-aanbevelingen (NIST SP 800-57 Part 1, Revision 5) en gerelateerde beveiligingsnormen, worden de volgende versleutelingsalgoritmen aanbevolen.

- 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

Over verouderde algoritmen

De RTMPS-functie ondersteunt tevens de volgende algoritmen omwille van de compatibiliteit, maar deze zijn verouderd op basis van de NIST-aanbevelingen (NIST SP 800-57 Part 1, Revision 5) en gerelateerde beveiligingsnormen, en kunnen in toekomstige versies worden verwijderd.

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

Compatibiliteit van de verbinding

De RTMPS-functie is ontworpen om beveiliging en compatibiliteit in evenwicht te brengen. Momenteel ondersteunen we verouderde algoritmen om de volgende redenen, maar we kunnen deze algoritmen in toekomstige versies verwijderen om de beveiliging te verbeteren.

- Om de RTMPS-streamingfunctie te kunnen gebruiken, moet u verbinding kunnen maken met diverse servers die de RTMPS-levering ondersteunen.
- Compatibiliteit met oudere systemen en legacy-servers moet worden behouden.
- Het wijzigen van de instellingen voor het versleutelingsalgoritme aan de server-kant is complex en niet alle gebruikers zijn bereid om te veranderen naar een veilige instelling.
- RTMPS-serverinstellingen worden vaak gedeeld met andere beveiligde services, dus is het noodzakelijk om rekening te houden met de gevolgen voor andere services op de server, en dat wijzigingen niet altijd eenvoudig zijn te implementeren.
- Om de interoperabiliteit in verschillende omgevingen te garanderen, is het noodzakelijk om een breed scala aan cryptografische algoritmen te ondersteunen.

Het versleutelingsalgoritme dat tijdens de RTMPS-verbinding wordt gebruikt, wordt bepaald tijdens automatische onderhandeling met de bestemmingsserver, en is dus afhankelijk van de instellingen op de server. Ondanks dat wij ons bewust zijn van de veiligheidsrisico's, geven we momenteel de voorkeur aan een brede compatibiliteit om tegemoet te komen aan de diverse behoeften van onze gebruikers.

Beveiligingsrisico's

Het gebruik van verouderde algoritmen, waaronder CBC en DHE, verhoogt het risico dat versleutelde gegevens worden ontsleuteld door een aanvaller, waardoor de gegevens tijdens het streamen kunnen worden onderschept.

Aanbevelingen voor een beveiligde verbinding

Als u de RTMPS-streamingfunctie gebruikt, controleert u van tevoren of de server waarmee u verbinding maakt, de aanbevolen versleutelingsalgoritmen ondersteunt. Wij adviseren u alleen de aanbevolen algoritmen inschakelt en alle niet-aanbevolen algoritmen uitschakelt aan de server-kant.

Verwijzingen

- 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).

TP1002071128