Funções SFTP/FTPES (FTPS)/RTMPS

Este Guia de Ajuda explica o protocolo de transferência de ficheiros (SFTP/FTPES (FTPS)) utilizado na função FTP e no protocolo de mensagens em tempo real sobre SSL (RTMPS) utilizado na função de transmissão de rede das câmaras digitais Sony.

Funções SFTP/FTPES (FTPS)/RTMPS

Sobre a função SFTP

A função SFTP suporta uma variedade de algoritmos de encriptação para transferências seguras de ficheiros. Para garantir a compatibilidade com uma ampla gama de servidores, são suportados vários algoritmos de encriptação, incluindo alguns que podem não estar em conformidade com as práticas de segurança recomendadas atualmente.

Algoritmos de encriptação suportados pela função SFTP

São suportados os seguintes algoritmos de encriptação.

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

Sobre os algoritmos de encriptação recomendados

Com base nas Recomendações NIST (NIST SP 800-57 Part 1, Revision 5) e nas normas de segurança relacionadas, recomendam-se os seguintes algoritmos de encriptação.

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

Sobre os algoritmos obsoletos

A função SFTP também suporta os seguintes algoritmos por razões de compatibilidade, porém, estes algoritmos estão obsoletos com base nas Recomendações NIST (NIST SP 800-57 Part 1, Revision 5) e nas normas de segurança relacionadas e podem ser removidos em versões futuras.

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

Compatibilidade de ligação

A função SFTP foi concebida para equilibrar segurança e compatibilidade. Atualmente, suportamos algoritmos obsoletos pelos seguintes motivos, mas podemos remover estes algoritmos em versões futuras para reforçar a segurança.

- Os fotógrafos e videógrafos freelance têm de se ligar a servidores operados por vários clientes.
- A compatibilidade com sistemas mais antigos e servidores legados deve ser mantida.
- Alterar as definições do algoritmo de encriptação no lado do servidor é complexo e nem todos os utilizadores estão preparados para mudar para uma definição segura.
- As definições do servidor SFTP são frequentemente partilhadas com outros serviços seguros, pelo que é necessário ter em conta o impacto noutros serviços do servidor, e as alterações nem sempre são fáceis de implementar.
- Para assegurar a interoperabilidade em diferentes ambientes, é necessário apoiar uma vasta gama de algoritmos criptográficos.

O algoritmo de encriptação utilizado durante a ligação SFTP é determinado pela negociação automática com o servidor de destino, pelo que depende das definições do servidor. Embora estejamos cientes dos riscos de segurança, atualmente damos prioridade a uma ampla compatibilidade, de modo a satisfazer as diversas necessidades dos nossos utilizadores.

Riscos de segurança

A utilização de algoritmos obsoletos aumenta a vulnerabilidade dos algoritmos baseados em SHA-1 e das chaves DSA para ataques de tipo “man-in-the-middle”, o risco de falsificação da identidade do servidor e a possibilidade de criptanálise com algoritmos de encriptação mais antigos (por exemplo, 3DES e variantes RC4), que podem expor dados em trânsito.

Recomendações para uma ligação segura

Ao utilizar a função de cliente SFTP, verifique previamente se o servidor ao qual se está a ligar suporta os algoritmos de encriptação recomendados. Recomendamos que ative apenas os algoritmos recomendados e desative os algoritmos não recomendados no lado do servidor.

Referências

- 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).

Funções SFTP/FTPES (FTPS)/RTMPS

Sobre a função FTPES (FTPS)

A função FTPES (FTPS) suporta uma variedade de algoritmos de encriptação para transferências seguras de ficheiros. Para garantir a compatibilidade com uma ampla gama de servidores, são suportados vários algoritmos de encriptação, incluindo alguns que podem não estar em conformidade com as práticas de segurança recomendadas atualmente.

Algoritmos de encriptação suportados pela função FTPES (FTPS)

São suportados os seguintes algoritmos de encriptação.

- 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

Sobre os algoritmos de encriptação recomendados

Com base nas Recomendações NIST (NIST SP 800-57 Part 1, Revision 5) e nas normas de segurança relacionadas, recomendam-se os seguintes algoritmos de encriptação.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Sobre os algoritmos obsoletos

A função FTPES (FTPS) também suporta os seguintes algoritmos por razões de compatibilidade, porém, estes algoritmos estão obsoletos com base nas Recomendações NIST (NIST SP 800-57 Part 1, Revision 5) e nas normas de segurança relacionadas e podem ser removidos em versões futuras.

- 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

Compatibilidade de ligação

A função FTPES (FTPS) foi concebida para equilibrar segurança e compatibilidade. Atualmente, suportamos algoritmos obsoletos pelos seguintes motivos, mas podemos remover estes algoritmos em versões futuras para reforçar a segurança.

- Os fotógrafos e videógrafos freelance têm de se ligar a servidores operados por vários clientes.
- A compatibilidade com sistemas mais antigos e servidores legados deve ser mantida.
- Alterar as definições do algoritmo de encriptação no lado do servidor é complexo e nem todos os utilizadores estão preparados para mudar para uma definição segura.
- As definições do servidor FTPES (FTPS) são frequentemente partilhadas com outros serviços seguros, pelo que é necessário ter em conta o impacto noutros serviços do servidor, e as alterações nem sempre são fáceis de implementar.
- Para assegurar a interoperabilidade em diferentes ambientes, é necessário apoiar uma vasta gama de algoritmos criptográficos.

O algoritmo de encriptação utilizado durante a ligação FTPES (FTPS) é determinado pela negociação automática com o servidor de destino, pelo que depende das definições do servidor. Embora estejamos cientes dos riscos de segurança, atualmente damos prioridade a uma ampla compatibilidade, de modo a satisfazer as diversas necessidades dos nossos utilizadores.

Riscos de segurança

A utilização de algoritmos obsoletos, incluindo CBC/DHE/RSA/SHA-1, aumenta o risco de que os dados encriptados possam ser desencriptados ou adulterados por um atacante, expondo os dados em trânsito.

Recomendações para uma ligação segura

Ao utilizar a função de cliente FTPES (FTPS), verifique previamente se o servidor ao qual se está a ligar suporta os algoritmos de encriptação recomendados. Recomendamos que ative apenas os algoritmos recomendados e desative os algoritmos não recomendados no lado do servidor.

Referências

- 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).

TP1002071117

Funções SFTP/FTPES (FTPS)/RTMPS

Sobre a função RTMPS

A função RTMPS suporta uma variedade de algoritmos de encriptação para transmissões RTMPS seguras. Para garantir a compatibilidade com uma vasta gama de servidores de destino, são suportados vários algoritmos de encriptação, incluindo alguns que podem não estar em conformidade com as melhores práticas de segurança atuais.

Algoritmos de encriptação suportados pela função RTMPS

São suportados os seguintes algoritmos de encriptação.

- 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

Sobre os algoritmos de encriptação recomendados

Com base nas Recomendações NIST (NIST SP 800-57 Part 1, Revision 5) e nas normas de segurança relacionadas, recomendam-se os seguintes algoritmos de encriptação.

- 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

Sobre os algoritmos obsoletos

A função RTMPS também suporta os seguintes algoritmos por razões de compatibilidade, porém, estes algoritmos estão obsoletos com base nas Recomendações NIST (NIST SP 800-57 Part 1, Revision 5) e nas normas de segurança relacionadas e podem ser removidos em versões futuras.

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

Compatibilidade de ligação

A função RTMPS foi concebida para equilibrar segurança e compatibilidade. Atualmente, suportamos algoritmos obsoletos pelos seguintes motivos, mas podemos remover estes algoritmos em versões futuras para reforçar a segurança.

- Para utilizar a função de transferência RTMPS, é necessário ligar-se a vários servidores que suportam a entrega de RTMPS.
- A compatibilidade com sistemas mais antigos e servidores legados deve ser mantida.
- Alterar as definições do algoritmo de encriptação no lado do servidor é complexo e nem todos os utilizadores estão preparados para mudar para uma definição segura.
- As definições do servidor RTMPS são frequentemente partilhadas com outros serviços seguros, pelo que é necessário ter em conta o impacto noutros serviços do servidor, e as alterações nem sempre são fáceis de implementar.
- Para assegurar a interoperabilidade em diferentes ambientes, é necessário apoiar uma vasta gama de algoritmos criptográficos.

O algoritmo de encriptação utilizado durante a ligação RTMPS é determinado pela negociação automática com o servidor de destino, pelo que depende das definições do servidor. Embora estejamos cientes dos riscos de segurança, atualmente damos prioridade a uma ampla compatibilidade, de modo a satisfazer as diversas necessidades dos nossos utilizadores.

Riscos de segurança

A utilização de algoritmos obsoletos, incluindo CBC e DHE, aumenta o risco de que os dados encriptados possam ser desencriptados ou adulterados por um atacante, expondo os dados que estão a ser transmitidos.

Recomendações para uma ligação segura

Ao utilizar a função de transmissão RTMPS, verifique previamente se o servidor ao qual se está a ligar suporta os algoritmos de encriptação recomendados. Recomendamos que ative apenas os algoritmos recomendados e desative os algoritmos não recomendados no lado do servidor.

Referências

- 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).

TP1002071118