

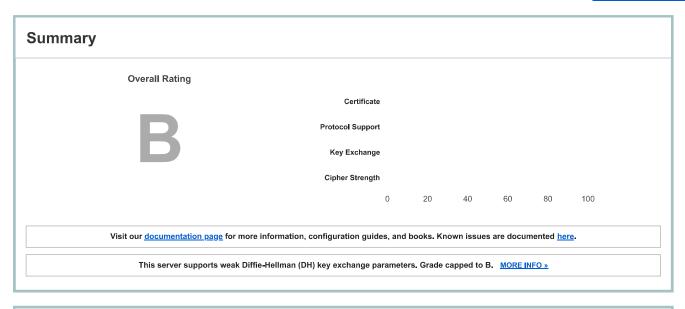
Home Projects Qualys.com Contact

You are here: $\underline{\text{Home}} > \underline{\text{Projects}} > \underline{\text{SSL Server Test}} > \text{www.uc.pt}$

SSL Report: www.uc.pt (193.137.200.184)

Assessed on: Mon, 19 Feb 2018 16:15:49 UTC | Hide | Clear cache

Scan Another »



Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

	apps.uc.pt		
Subject	Fingerprint SHA256: 965a18e49bf2047a886fcb12755ec9378cc0814d992e14afdf609cac73002898		
	Pin SHA256: Q44v0nVLQaES4Jda+JrbEc27OIkAsiZ+ohV3em8dI+Y=		
Common names	apps.uc.pt		
Alternative names	apps.uc.pt www.uc.pt api.uc.pt		
Serial Number	0fce3e7466cb39378878e7ccf54ea920		
Valid from	Tue, 29 Dec 2015 00:00:00 UTC		
Valid until	Wed, 02 Jan 2019 12:00:00 UTC (expires in 10 months and 13 days)		
Key	RSA 2048 bits (e 65537)		
Weak key (Debian)	No		
	TERENA SSL CA 3		
Issuer	AIA: http://cacerts.digicert.com/TERENASSLCA3.crt		
Signature algorithm	SHA256withRSA		
Extended Validation	No		
Certificate Transparency	No		
OCSP Must Staple	No		
	CRL, OCSP		
Revocation information	CRL: http://crl3.digicert.com/TERENASSLCA3.crl		
	OCSP: http://ocsp.digicert.com		
Revocation status	Good (not revoked)		
DNS CAA	No (<u>more info</u>)		
Trusted	Yes		
Trusteu	Mozilla Apple Android Java Windows		



Additional Certificates (if supplied)

Certificates provided	2 (2646 bytes)
Chain issues	None
#9	

Additional Certificates (if supplied) TERENA SSL CA 3 Subject Fingerprint SHA256: beb8efe9b1a73c841b375a90e5fff8048848e3a2af66f6c4dd7b938d6fe8c5d8 Pin SHA256: 8651wEkMkH5ftlaLp57oqmx3KHTFzDgp7ZeJXR0ToBs= Valid until Mon, 18 Nov 2024 12:00:00 UTC (expires in 6 years and 8 months) Key RSA 2048 bits (e 65537) Issuer DigiCert Assured ID Root CA Signature algorithm SHA256withRSA



Certification Paths +

Click here to expand

Configuration



Protocols TLS 1.3 No TLS 1.2 Yes TLS 1.1 Yes TLS 1.0 Yes SSL 3 No SSL 2 No For TLS 1.3 tests, we currently support draft version 18.



Cipher Suites

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (exce39) ECDH secq256r1 (eq. 3072 bits RSA) FS TLS_ECDHE_RSA_WITH_AES_256_GCBC_SHA384 (exce28) ECDH secq256r1 (eq. 3072 bits RSA) FS TLS_DHE_RSA_WITH_AES_256_GCBC_SHA384 (exce28) ECDH secq256r1 (eq. 3072 bits RSA) FS TLS_DHE_RSA_WITH_AES_256_GCBC_SHA384 (exce28) ECDH secq256r1 (eq. 3072 bits RSA) FS TLS_DHE_RSA_WITH_AES_256_GCBC_SHA384 (exce28) ECDH secq256r1 (eq. 3072 bits RSA) FS TLS_DHE_RSA_WITH_AES_256_GCBC_SHA256 (exc6b) DH 1024 bits FS WEAK TLS_DHE_RSA_WITH_AES_256_GCBC_SHA (exce39) DH 1024 bits FS WEAK TLS_DHE_RSA_WITH_AES_256_GCBC_SHA (exce39) DH 1024 bits FS WEAK TLS_RSA_WITH_AES_256_GCBC_SHA384 (exce39) WEAK TLS_RSA_WITH_AES_256_GCBC_SHA384 (exce39) WEAK TLS_RSA_WITH_AES_256_GCBC_SHA384 (exce35) WEAK TLS_RSA_WITH_AES_256_GCBC_SHA46 (exce35) WEAK TLS_RSA_WITH_AES_256_GCBC_SHA46 (exce35) WEAK TLS_RSA_WITH_AES_128_GCBC_SHA46 (exce37) ECDH secq256r1 (eq. 3072 bits RSA) FS TLS_ECDHE_RSA_WITH_AES_128_GCBC_SHA46 (exce313) ECDH secq256r1 (eq. 3072 bits RSA) FS TLS_ECDHE_RSA_WITH_AES_128_GCBC_SHA46 (exce313) ECDH secq256r1 (eq. 3072 bits RSA) FS TLS_DHE_RSA_WITH_AES_128_GCBC_SHA566 (exce37) DH 1024 bits FS WEAK TLS_RSA_WITH_AES_128_GCBC_SHA566 (exce37) WEAK TLS_RSA_WITH_AES_128_GCBC_SHA566 (exce37) WEAK TLS_RSA_WITH_AES_128_GCBC_SHA6641) WEAK TLS_RSA_WITH_AES_128_GCBC_SHA6641) WEAK TLS_RSA_WITH_AES_128_GCBC_SHA6641) WEAK TLS_RSA_WITH_AES_128_GCBC_SHA6641) WEAK TLS_PLE_RSA_WITH_3DES_EDE_GCBC_SHA6641) WEAK TLS_DHE_RSA_WITH_3DES_EDE_GCBC_SHA6641) WEAK TLS_DHE_RSA_WITH_3DES_EDE_GCBC_SHA6641) WEAK TLS_DHE_RSA_WITH_3DES_EDE_GCBC_SHA6641) WEAK		
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA884 (exce28) ECDH secp256f1 (eq. 3072 bits RSA) FS 2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (exce14) ECDH secp256f1 (eq. 3072 bits RSA) FS 2 TLS_DHE_RSA_WITH_AES_256_CBC_SHA884 (exce14) ECDH secp256f1 (eq. 3072 bits RSA) FS 2 TLS_DHE_RSA_WITH_AES_256_CBC_SHA984 (exce14) ECDH secp256f1 (eq. 3072 bits RSA) FS 2 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (exceb) DH 1024 bits FS WEAK 2 TLS_DHE_RSA_WITH_AES_256_CBC_SHA984 (exce14) ECDH secp256f1 (eq. 3072 bits RSA) FS 2 TLS_DHE_RSA_WITH_AES_256_CBC_SHA984 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_RSA_WITH_AES_256_CBC_SHA984 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (exce27) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA945 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA956 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA956 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA956 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA956 (exce13) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA956 (exce12) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA956 (exce12) ECDH secp256f1 (eq. 3072 bits RSA) FS 2 TLS_RSA_WITH_AES_128_CBC_SHA956 (exce12) ECDH secp256f1 (eq. 3072 bits RSA) FS 3 TLS_RSA_WITH_AES_128_CBC_SHA956 (exce12) ECDH secp256f1 (eq. 3072 bits RSA) FS 4 TLS_RSA_WITH_AES_128_CBC_SHA956 (exce12) ECDH secp256f1 (eq. 3072 bits RSA) FS 4 TLS_RSA_WITH_AES_128_CBC_SHA956 (exce12) ECDH secp256f1 (eq. 3072 bits RSA) FS 4 TLS_RSA_WITH_AES_128_CBC_SHA956 (exce12) ECDH secp256f1 (eq. 3072 bits RSA) FS 4 TLS_RSA_WITH_AES_12	# TLS 1.2 (suites in server-preferred order)	E
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (exceld) ECDH secp25611 (eq. 3072 bits RSA) FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA(26x6b) DH 1024 bits FS WEAK 2. TLS_DHE_RSA_WITH_AES_256_CBC_SHA(26x6b) DH 1024 bits FS WEAK 2. TLS_DHE_RSA_WITH_AES_256_CBC_SHA (ex39) DH 1024 bits FS WEAK 2. TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (ex38) DH 1024 bits FS WEAK 2. TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (ex38) DH 1024 bits FS WEAK 2. TLS_RSA_WITH_AES_256_CBC_SHA(ex38) WEAK 2. TLS_RSA_WITH_AES_256_CBC_SHA(26x3d) WEAK 2. TLS_RSA_WITH_AES_256_CBC_SHA(26x3d) WEAK 2. TLS_RSA_WITH_AES_256_CBC_SHA(26x3d) WEAK 2. TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 3. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x27) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 4. TLS_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 4. TLS_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 4. TLS_RSA_WITH_AES_128_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 4. TLS_RSA_WITH_3DES_EDE_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 4. TLS_RSA_WITH_3DES_EDE_CBC_SHA(26x26f) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 4. TLS_RSA_WITH_3DES_EDE_	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (exef) DH 1024 bits FS WEAK 2. TLS_DHE_RSA_WITH_AES_256_GBC_SHA(exeb) DH 1024 bits FS WEAK 2. TLS_DHE_RSA_WITH_AES_256_GBC_SHA(exis) DH 1024 bits FS WEAK 2. TLS_DHE_RSA_WITH_CAMELLIA_256_GBC_SHA (exis) DH 1024 bits FS WEAK 2. TLS_DHE_RSA_WITH_CAMELLIA_256_GBC_SHA(exis) DH 1024 bits FS WEAK 2. TLS_RSA_WITH_AES_256_GCM_SHA384 (exis) WEAK 2. TLS_RSA_WITH_AES_256_GBC_SHA(exis) WEAK 2. TLS_RSA_WITH_AES_256_GBC_SHA(exis) WEAK 2. TLS_RSA_WITH_AES_256_GBC_SHA(exis) WEAK 2. TLS_RSA_WITH_AES_256_GBC_SHA(exis) WEAK 2. TLS_RSA_WITH_AES_128_GCM_SHA256 (exis) WEAK 2. TLS_RSA_WITH_AES_128_GCM_SHA256 (exis) WEAK 2. TLS_RSA_WITH_AES_128_GCM_SHA256 (exis) WEAK 2. TLS_RSA_WITH_AES_128_GCM_SHA256 (exis) WEAK 2. TLS_BCDHE_RSA_WITH_AES_128_GCM_SHA256 (exis) DH 1024 bits FS WEAK 3. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (exis) DH 1024 bits FS WEAK 4. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (exis) WEAK 4. TLS_RSA_WITH_AES_128_GCM_SHA256 (exis) WEAK 4. TLS_TLS_CHE_RSA_WITH_3DES_EDE_CBC_SHA (exis) DH 1024 bits FS WEAK 4. TLS_TLS_CHE_RSA_WITH_3DES_EDE_CBC_SHA (exis) DH 1024 bits FS WEAK 4. TLS_TLS_TLS_TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (exis) DH 1024 bits FS WEAK 4. TLS_TLS_TLS_TLS_TLS_DES_EDE_CBC_SHA (exis) WEAK 4. TLS_TLS_TLS_TLS_TLS_TLS_TLS_TLS_TLS_TLS_	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA(ex39) DH 1024 bits_FS_WEAK 2. TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(ex39) DH 1024 bits_FS_WEAK 2. TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(ex38) DH 1024 bits_FS_WEAK 2. TLS_RSA_WITH_AES_256_CBC_SHA9348 (ex34) WEAK 2. TLS_RSA_WITH_AES_256_CBC_SHA256 (ex3d) WEAK 2. TLS_RSA_WITH_AES_256_CBC_SHA(ex35) WEAK 2. TLS_RSA_WITH_AES_256_CBC_SHA(ex35) WEAK 2. TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (ex34) WEAK 2. TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (ex34) WEAK 2. TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(ex34) WEAK 2. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (exce27) ECDH secp256r1 (eq. 3072 bits RSA) FS 3. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 3. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_AES_128_CBC_SHA(exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_AES_128_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_SDES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_SDES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_SDES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_SDES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_SDES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS 4. TLS_RSA_WITH_SDES_EDE_CBC_SHA (exce12) WEAK	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (exa9) DH 1024 bits FS WEAK 2 TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (exa8) DH 1024 bits FS WEAK 2 TLS_RSA_WITH_AES_256_GCM_SHA334 (exa9) WEAK 2 TLS_RSA_WITH_AES_256_CBC_SHA256 (exa3) WEAK 2 TLS_RSA_WITH_AES_256_CBC_SHA (exa9) WEAK 2 TLS_RSA_WITH_AES_256_CBC_SHA (exa9) WEAK 2 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (exa9) WEAK 2 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (exa9) WEAK 2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (exce27) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (exce27) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce013) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce013) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce013) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce013) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce013) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exa3) DH 1024 bits FS WEAK 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exa3) DH 1024 bits FS WEAK 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exa45) DH 1024 bits FS WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (exa5) DH 1024 bits FS WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (exa5) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (exa1) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (exa1) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (exce11) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_LCDHE_RSA_WITH_3DES_EDE_CBC_SHA (exce112) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_LCDHE_RSA_WITH_3DES_EDE_CBC_SHA (exce112) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_LCDHE_RSA_WITH_3DES_EDE_CBC_SHA (exce112) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_LCDHE_RSA_WITH_3DES_EDE_CBC_SHA (exce112) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_LCDHE_RSA_WITH_3DES_EDE_CBC_SHA (exce112) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits FS WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (ex88) DH 1024 bits FS WEAK 2 TLS_RSA_WITH_AES_256_CBC_SHA384 (ex34) WEAK 2 TLS_RSA_WITH_AES_256_CBC_SHA256 (ex3d) WEAK 2 TLS_RSA_WITH_AES_256_CBC_SHA (ex35) WEAK 2 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (ex34) WEAK 2 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (ex34) WEAK 2 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (ex34) WEAK 2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (exce27) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (exce27) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce31) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce31) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce31) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce31) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exa3) DH 1024 bits FS WEAK 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exa3) DH 1024 bits FS WEAK 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exa5) DH 1024 bits FS WEAK 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exa5) DH 1024 bits FS WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (ex26) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (ex27) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (ex27) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (ex21) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (ex21) WEAK 1 TLS_CDHE_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 1 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits FS WEAK	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (exed) WEAK 2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (ex3d) WEAK 21 TLS_RSA_WITH_AES_256_CBC_SHA (ex35) WEAK 22 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (ex35) WEAK 23 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (ex34) WEAK 24 TLS_RSA_WITH_AES_128_GCM_SHA256 (exc92f) ECDH secp256r1 (eq. 3072 bits RSA) FS 25 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (exc927) ECDH secp256r1 (eq. 3072 bits RSA) FS 26 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (exc913) ECDH secp256r1 (eq. 3072 bits RSA) FS 27 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exc913) ECDH secp256r1 (eq. 3072 bits RSA) FS 28 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (exc92) DH 1024 bits FS WEAK 29 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (exc92) DH 1024 bits FS WEAK 30 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (ex33) DH 1024 bits FS WEAK 31 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (ex45) DH 1024 bits FS WEAK 32 TLS_RSA_WITH_AES_128_CBC_SHA256 (ex9c) WEAK 33 TLS_RSA_WITH_AES_128_CBC_SHA256 (ex3c) WEAK 34 TLS_RSA_WITH_AES_128_CBC_SHA (ex2f) WEAK 35 TLS_RSA_WITH_AES_128_CBC_SHA (ex2f) WEAK 36 TLS_RSA_WITH_AES_128_CBC_SHA (ex2f) WEAK 37 TLS_RSA_WITH_AES_128_CBC_SHA (ex2f) WEAK 38 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 39 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 40 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 41 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 42 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 43 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 44 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 45 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 45 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 46 TLS_RSA_WITH_3DES_EDE_CBC_SHA (ex16) DH 1024 bits FS WEAK 47 TLS_11 (suites in server-preferred order)	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 1024 bits FS WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK 2 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256f1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc013) DH 1024 bits FS WEAK 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc013) DH 1024 bits FS WEAK 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc013) DH 1024 bits FS WEAK 1 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0xc012) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (0xc012) WEAK 1 TLS_RSA_WITH_AES_128_CBC_SHA (0xc012) ECDH secp256f1 (eq. 3072 bits RSA) FS WEAK 1 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256f1 (eq. 3072 bits RSA) FS WEAK 1 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256f1 (eq. 3072 bits RSA) FS WEAK 1 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256f1 (eq. 3072 bits RSA) FS WEAK 1 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256f1 (eq. 3072 bits RSA) FS WEAK 1 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256f1 (eq. 3072 bits RSA) FS WEAK 1 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256f1 (eq. 3072 bits RSA) FS WEAK	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (ex84) WEAK TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (exce2f) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (exce27) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (exce13) ECDH secp256r1 (eq. 3072 bits RSA) FS 1 TLS_RSA_WITH_AES_128_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_CHE_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r1 (eq. 3072 bits RSA) FS TLS_RSA_WITH_3DES_EDE_CBC_SHA (exce12) ECDH secp256r	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS 11LS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS 11LS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS 11LS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 11LS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 11LS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA (0x41) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA (0x41) WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (0x41) WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (0x41) WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (0x6012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (0x616) DH 1024 bits FS WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (0x016) DH 1024 bits FS WEAK	TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS 11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS 12 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x9e) DH 1024 bits FS WEAK 13 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits FS WEAK 14 TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK 15 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS WEAK 16 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS WEAK 17 TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 18 TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK 19 TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 10 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x2f) WEAK 11 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK 12 TLS_RSA_WITH_SDES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11 TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11 TLS_CDHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) WEAK	250
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS 11LS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS WEAK 11LS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 11LS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK 11LS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11LS_CDHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (exse) DH 1024 bits FS WEAK 11S_DHE_RSA_WITH_AES_128_CBC_SHA256 (exser) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_AES_128_CBC_SHA (exss) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (exss) DH 1024 bits FS WEAK 11LS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (exser) DH 1024 bits FS WEAK 11LS_RSA_WITH_AES_128_GCM_SHA256 (exser) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA256 (exser) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA (exser) WEAK 11LS_RSA_WITH_AES_128_CBC_SHA (exser) WEAK 11LS_RSA_WITH_CAMELLIA_128_CBC_SHA (exser) WEAK 11LS_CDHE_RSA_WITH_3DES_EDE_CBC_SHA (exser) ECDH secp256f1 (eq. 3072 bits RSA) FS WEAK 11LS_CDHE_RSA_WITH_3DES_EDE_CBC_SHA (exser) DH 1024 bits FS WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (exser) WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (exser) WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (exser) WEAK 11LS_RSA_WITH_3DES_EDE_CBC_SHA (exser) WEAK	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x33) DH 1024 bits FS WEAK TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS WEAK TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK TLS_RSA_WITH_AES_128_GCBC_SHA256 (0x3c) WEAK TLS_RSA_WITH_AES_128_CBC_SHA256 (0x2f) WEAK TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0x41) WEAK TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS WEAK TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK TLS_RSA_WITH_AES_128_CBC_SHA(0x2f) WEAK TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x16) WEAK	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits FS WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS WEAK 11S_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 11S_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK 11S_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 11S_RSA_WITH_CAMELLIA_128_CBC_SHA (0x2f) WEAK 11S_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK 11S_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK 11S_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK 11S_RSA_WITH_3DES_EDE_CBC_SHA (0x3) WEAK 11S_RSA_WITH_3DES_EDE_CBC_SHA (0x3) WEAK	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits FS WEAK	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0x012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK **TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK #TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45) DH 1024 bits FS WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK #TLS_1.1 (suites in server-preferred order)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK # TLS 1.1 (suites in server-preferred order)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK # TLS 1.1 (suites in server-preferred order)	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK #TLS 1.1 (suites in server-preferred order)	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) WEAK	128
# TLS 1.1 (suites in server-preferred order)	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	112
# TLS 1.1 (suites in server-preferred order)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS WEAK	112
	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
#TLS 1.0 (suites in server-preferred order)	# TLS 1.1 (suites in server-preferred order)	+
	#TLS 1.0 (suites in server-preferred order)	+



Handshake Simulation

Android 2.3.7 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Chrome 57 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 53 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 8 / XP No FS ¹ No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
<u>IE 8-10 / Win 7</u> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
<u>IE 11 / Win 7</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
<u>IE 11 / Win 8.1</u> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
· · · · · · · · · · · · · · · · · · ·		120 Hz Hup/III	
<u>IE 11 / Win 10</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>IE 11 / Win 10</u> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>IE 11 / Win 10</u> R <u>Edge 13 / Win 10</u> R	RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
IE 11 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R	RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
IE 11 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI ²	RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
IE 11 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25	RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31	RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256) RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
E 11 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI ² Java 7u25 Java 8u31 OpenSSL 0.9.8y.	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.11 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1l R OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
IE 11 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1l R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1I R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1l R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1I R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1I R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1l R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 7 / iOS 7.1 R Safari 7 / OS X 10.9 R Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1I R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.04 / OS X 10.8.4 R Safari 7 / iOS 7.1 R Safari 7 / iOS 7.1 R Safari 8 / iOS 8.4 R Safari 8 / iOS 8.4 R Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1I R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / IOS 6.0.1 Safari 6 / IOS 7.1 R Safari 7 / IOS 7.1 R Safari 8 / IOS 8.4 R Safari 8 / IOS 8.4 R Safari 8 / IOS 9 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1l R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R Safari 7 / OS X 10.9 R Safari 8 / iOS 8.4 R Safari 8 / iOS 9 R Safari 9 / iOS 9 R Safari 9 / iOS 9 R Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1I R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R Safari 7 / iOS 7.1 R Safari 8 / iOS 8.4 R Safari 8 / iOS 8.4 R Safari 9 / iOS 9 R Safari 9 / iOS 9 R Safari 9 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 http/1.1 TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI 2 Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.1I R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / IOS 6.0.1 Safari 6 / IOS 7.1 R Safari 7 / OS X 10.9 R Safari 8 / IOS 8.4 R Safari 8 / IOS 8.4 R Safari 9 / IOS 9 R Safari 9 / IOS 9 R Safari 10 / IOS 10 R Safari 10 / IOS 10 R Safari 10 / IOS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 > http/1.1 TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 13 / Win 10 R Edge 13 / Win 10 R Edge 13 / Win Phone 10 R Java 6u45 No SNI ² Java 7u25 Java 8u31 OpenSSL 0.9.8y. OpenSSL 1.0.11 R OpenSSL 1.0.2e R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6 / iOS 7.1 R Safari 7 / iOS 7.1 R Safari 8 / iOS 8.4 R Safari 8 / iOS 8.4 R Safari 9 / iOS 9 R Safari 9 / iOS 9 R Safari 10 / iOS 10 R Safari 10 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.2 > http/1.1 TLS 1.2 > http/1.1 TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)

<u>IE 6 / XP</u> No FS ¹ No SNI ² Protocol mismatch (not simulated)

_

 $^{(1) \} Clients \ that \ do \ not \ support \ Forward \ Secrecy \ (FS) \ are \ excluded \ when \ determining \ support \ for \ it.$

 $^{(2) \} No \ support \ for \ virtual \ SSL \ hosting \ (SNI). \ Connects \ to \ the \ default \ site \ if \ the \ server \ uses \ SNI.$

Handshake Simulation

- (3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.
- (R) Denotes a reference browser or client, with which we expect better effective security.
- (All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
- (All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.



Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Weak key exchange WEAK
ALPN	No
NPN	Yes http://1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	secp256r1
SSL 2 handshake compatibility	Yes



HTTP Requests







Miscellaneous

Test date	Mon, 19 Feb 2018 16:12:48 UTC
Test duration	181.397 seconds
HTTP status code	200
HTTP server signature	nginx/1.10.2
Server hostname	-

SSL Report v1.30.8

Copyright © 2009-2018 Qualys, Inc. All Rights Reserved.

Terms and Conditions

Qualys is the leading provider of integrated infrastructure security, cloud infrastructure security, endpoint security, devsecops, compliance and web app security solutions.