

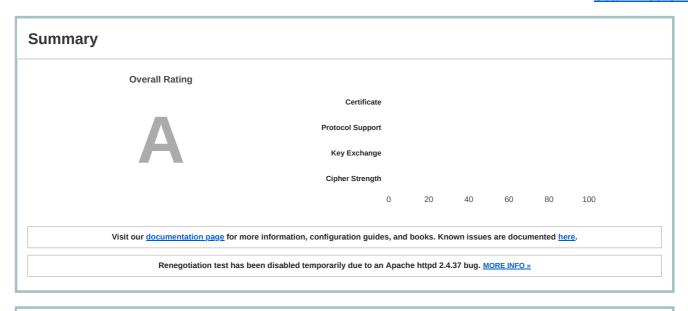
Home Projects Qualys Free Trial Contact

You are here: <u>Home</u> > <u>Projects</u> > <u>SSL Server Test</u> > www.flowtraders.com

SSL Report: www.flowtraders.com (83.217.84.138)

Assessed on: Mon, 18 Feb 2019 16:42:00 UTC | Hide | Clear cache

Scan Another »



Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	www.flowtraders.com Fingerprint SHA256: b03185f78ebb513efca1569c38127aba0d9f9443545e17c0e391d098612d4e66 Pin SHA256: MyVQd8WDsF/n02IOBa/j7ZblfR765DYdr9cf3B3KaK4=
Common names	www.flowtraders.com
Alternative names	www.flowtraders.com flowtraders.com
Serial Number	00b4074297a14557080a370378d58850a7
Valid from	Fri, 18 Jan 2019 00:00:00 UTC
Valid until	Sat, 18 Jan 2020 23:59:59 UTC (expires in 11 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Domain Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	3 (4605 bytes)
Chain issues	Contains anchor
#2	
	Sectigo RSA Domain Validation Secure Server CA
Subject	Fingerprint SHA256: 7fa4ff68ec04a99d7528d5085f94907f4d1dd1c5381bacdc832ed5c960214676
	Pin SHA256: 4a6cPehI7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng=

Additional Certificates (if supplied) Valid until Tue, 31 Dec 2030 23:59:59 UTC (expires in 11 years and 10 months) Key RSA 2048 bits (e 65537) USERTrust RSA Certification Authority Issuer Signature algorithm SHA384withRSA USERTrust RSA Certification Authority In trust store Subject Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2 Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= Valid until Mon, 18 Jan 2038 23:59:59 UTC (expires in 18 years and 11 months) Key RSA 4096 bits (e 65537) USERTrust RSA Certification Authority Self-signed Issuer Signature algorithm SHA384withRSA



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 only support RFC 8446.



Cipher Suites

# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
# TLS 1.1 (suites in server-preferred order)	+
# TLS 1.0 (suites in server-preferred order)	+

+



Martine (2.0.2.1 to solid	Handshake Simulation			
### And Applications	Android 2.3.7 No SNI ²	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS
Control of 2.2 Pai 2.000 (SPA 2000 (SPA 20	Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
ADMINISTRATE NA COMMINISTRATION T.S. COMP. PAS. WITH LAS. 260, COM. SHAW EXCHANGED ITS ADMINISTRATE NA COMMINISTRATION T.S. T.S. ECONE. PAS. WITH LAS. 260, COM. SHAWS EXCHANGED ITS ADMINISTRATION T.S. T.S. T.S. T.S. T.S. ECONE. PAS. WITH LAS. 260, COM. SHAWS EXCHANGED ITS ADMINISTRATION T.S. T.S. T.S. T.S. T.S. T.S. T.S. T.S. ADMINISTRATION T.S. T.S. T.S. T.S. T.S. T.S. T.S. T.S. T.S. ADMINISTRATION T.S. T.S. T.S. T.S. T.S. T.S. T.S. T.S. T.S. ADMINISTRATION T.S. ADMINISTRATION T.S. T	Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Android 4.2 Res 2948 (SHAXS) 1.5.1.2 TLS ECONE RRA WITH AES 226 DCM SHAXSE ECON erequion 149 Android 5.0.0 PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 120 DCM SHAXSE ECON erequion 149 Android 5.0.0 PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 120 DCM SHAXSE ECON erequion 149 Android 5.0.0 PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 149 Build Jane 2015 PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 Build Jane 2015 PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 Chrome 69 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 Chrome 69 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 Chrome 50 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 Chrome 50 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 256 DCM SHAXSE ECON erequion 159 FERENCE 21 /Win 7 R PM A 2948 (SHAXSE) 1.5.1.2 NB/LL TLS ECONE RRA WITH AES 25	Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
AMERICADO RES ADMINISTRATO TILS 12 TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TEST AMERICADO TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TEST AMERICAN TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TEST AMERICAN TILS 12 TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS 12 > INDITED TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS TILD TILD TILD TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS TILD TILD TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS TILD TILD TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS TILD TILD TILS ECONE REAL WITH LARS 1781 COCAL SMAZZAGE FOOT HANDSON TILS TILD TILD TILS ECON	Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
ADMINISTED R9A 2008 (SIMASS) TLS 12 > http://li> ADMINISTED R9A 2008 (SIMASS) TLS 12 >	Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Author 7:0 Read And (SHA259) TIS 12 > http:// TIS_ECOHE_RSA_WITH_AES_256_GCG_SHA_ECOH sequition is Balled and 2015 Read And 2015 Read And (SHA259) TIS 12 > http:// TIS_ECOHE_RSA_WITH_AES_26_GCG_SHA_ECOH sequition is Billing/below/win_and 2015 Read And (SHA259) TIS 12 > http:// TIS_ECOHE_RSA_WITH_AES_26_GCG_SHA_ECOH sequition is Billing/below/win_and 2015 Read And (SHA259) TIS 12 > http:// TIS_ECOHE_RSA_WITH_AES_26_GCG_SHA_ECOH sequition is Billing/below/win_and 2015 Read And (SHA259) TIS 12 > http:// TIS_ECOHE_RSA_WITH_AES_26_GCG_SHA388 ECOH sequition is Billing/below/win_and and and and and and and and and and	Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Babb_Jan_2015 R9A 2048 (RHA298) TLS 1.0 TLS_ECONE_RSA_WITH_ASS_266_CBC_SHA RECHARGEDIST IS	Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
BasePlaceview, Jan 2015	Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 89 / XP SP2	Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Chrome 69 / Win 7 R RS A2048 (SNA258) TI.S 1.2 > http://lil. TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS Firefox 31.3.0 ESR / Win 7 RS A2048 (SNA258) TI.S 1.2 > http://lil. TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS Firefox 41 / Win 7 R RS A2048 (SNA258) TI.S 1.2 > http://lil. TI.S ECDHE_RSA_WITH_AES_128_GCM_SNA384 ECDH secq25661 FS Firefox 47 / Win 7 R RS A2048 (SNA258) TI.S 1.2 > http://lil. TI.S ECDHE_RSA_WITH_AES_128_GCM_SNA384 ECDH secq25661 FS Firefox 47 / Win 7 R RS A2048 (SNA258) TI.S 1.2 > http://lil. TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS Firefox 62 / Win 7 R RS A2048 (SNA258) TI.S 1.2 > http://lil. TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS Googlehe Feb 2018 RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS Firefox 62 / Win 7 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 7 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 7 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA 2048 (SNA258) TI.S 1.2 TI.S ECDHE_RSA_WITH_AES_286_GCM_SNA384 ECDH secq25661 FS FIREFOX MIN 2 R RSA	BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 20 I Win 10 RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 31 3.0 ESR / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 41 3.0 ESR / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 42 / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 42 / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 42 / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 42 / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 52 / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 52 / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 52 / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 52 / Win 7 R RSA 2046 (SHA256) TLS 12 > http://li> Fizefox 52 / Win 7 R RSA 2046 (SHA256) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA256) TLS 10 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA256) TLS 10 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA256) TLS 10 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA256) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA256) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA256) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA256) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA266 ECON secption FS RSA 2046 (SHA256) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA266 ECON secption FS RSA 2046 (SHA266) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA266 ECON secption FS RSA 2046 (SHA266) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA266 ECON secption FS RSA 2046 (SHA266) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA266 ECON secption FS RSA 2046 (SHA266) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA266 ECON secption FS RSA 2046 (SHA266) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA266) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA264 ECON secption FS RSA 2046 (SHA266) TLS 12 TLS ECONE, RSA WITH ASS, 266 (CSC_SHA ECON secption FS RSA 2046 (SHA26	Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Findbax 31.3.0 ESR / Win 7	Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 47 / Win 7 R	Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 49 / XP SP2	Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
File Company File	Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Coopelation Feb 2018 RSA 2048 (SHA258) TLS 1.2 TLS_ECOHE_RSA_WITH_AES_256_GCM_SHA884 ECOH secq25661 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
E. F. Visita RSA 2048 (SHA258) TLS 1.0 TLS ECDHE RSA_WITH_AES_256_CBC_SHA ECDH sexp256r1 FS	Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
E. F. Visita RSA 2048 (SHA256) TLS 1.0 TLS ECDHE RSA_WITH_AES_256_CBC_SHA ECDH sexp256r1 FS	Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	
EB 1/Win 1 R RSA 2048 (SHA256) TLS 1.0 TLS ECOHE_RSA_WITH_AES_256_CBC_SHA ECOH seep256f1 FS		RSA 2048 (SHA256)	TLS 1.0	
EB.10 Win 7 R	IE 8 / XP No FS ¹ No SNI ²	Server sent fatal ale	rt: handshake_ failure	
				TLS ECDHE RSA WITH AES 256 CBC SHA ECDH secp256r1 FS
IE 10 / Win Phone 8.0				
IE 11 / Win Phone 8.1 R				
In the content of t		RSA 2048 (SHA256)		
E11 Win 10 R	IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	
Edge 15 / Win 10 R RSA 2048 (SHA256) TLS 1.2 > http/l.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Edge 13 / Win Phone 10 R RSA 2048 (SHA256) TLS 1.2 > http/l.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Java 6u45 No SNI 2 Client does not support DH parameters > 1024 bits RSA 2048 (SHA256) TLS 1.0 TLS_DHE_RSA_WITH_AES_128_GBC_SHA DH 2048 Java 7u25 RSA 2048 (SHA256) TLS 1.0 TLS_DHE_RSA_WITH_AES_128_GBC_SHA ECDH secp256r1 FS Java 8u161 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS QpenSSL 0.9.BY RSA 2048 (SHA256) TLS 1.0 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS QpenSSL 1.0.11 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS QpenSSL 1.0.22 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 6.10S 6.0.1 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 6.10S 6.0.1 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_GCC_SHA ECDH secp256r1 FS Safari 7.10S 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCC_SHA ECDH secp256r1 FS Safari 7.10S 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCC_SHA384 ECDH secp256r1 FS Safari 7.10S 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCC_SHA384 ECDH secp256r1 FS Safari 8.10S 8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCC_SHA384 ECDH secp256r1 FS Safari 8.10S 8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCC_SHA384 ECDH secp256r1 FS Safari 8.10S 8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCC_SHA384 ECDH secp256r1 FS Safari 9.10S 9. R RSA 2048 (SHA256) TLS 1.2 > http://.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 9.10S 9. R RSA 2048 (SHA256) TLS 1.2 > http://.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10.10S 10 R RSA 2048 (SHA256) TLS 1.2 > http://.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10.10S 10 R RSA 2048 (SHA256	IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	
Client does not support DH parameters > 10.24 bits RSA 2048 (SHA256) TLS 1.0 TLS _ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS		RSA 2048 (SHA256)	•	
Client does not support DH parameters > 1024 bits RSA 2048 (SHA256) TLS 1.0 TLS DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 Java 7u/25	Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)		TLS ECDHE RSA WITH AES 256 GCM SHA384 ECDH secp256r1 FS
RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS Java 8u161		Client does not supp	oort DH parameters > 1	
Java 8u161 RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS OpenSSL 0.9.8y RSA 2048 (SHA256) TLS 1.0 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS OpenSSL 1.0.1l R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS OpenSSL 1.0.2e R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 5.1.9 / OS X 10.6.8 RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS Safari 6 / IOS 6.0.1 RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 84 ECDH secp256r1 FS Safari 7 / IOS X 10.8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS X 10.11 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECD	Java 6u45 No SNI ²	RSA 2048 (SHA256)	TLS 1.0 TLS_DHE_RSA	_WITH_AES_128_CBC_SHA DH 2048
OpenSSL 0.9.8y RSA 2048 (SHA256) TLS 1.0 TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 2048 FS OpenSSL 1.0.1l R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS OpenSSL 1.0.2e R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 5.1.9 / OS X 10.6.8 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS Safari 6 / IOS 6.0.1 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS X 10.8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS 8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS X 10.11 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<u>Java 7u25</u>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
OpenSSL 1.0.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS OpenSSL 1.0.2e R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 5.1.9 / OS X 10.6.8 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS Safari 6 / IOS 6.0.1 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS X 10.8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS X 10.11 R RSA 2048 (SHA256) TLS 1.2 > http/1.1	<u>Java 8u161</u>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.2e R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 5.1.9 / OS X 10.6.8 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS Safari 6 / IOS 6.0.1 RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS X 10.8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS <td>OpenSSL 0.9.8y</td> <td>RSA 2048 (SHA256)</td> <td>TLS 1.0</td> <td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 2048 FS</td>	OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 2048 FS
Safari 5.1.9 / OS X 10.6.8 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS Safari 6 / IOS 6.0.1 RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 6 / IOS 6.0.1 RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / IOS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS 2 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS 3 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_2	OpenSSL 1.0.1I R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 6 / iOS 6.0.1 RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 6.0.4 / OS X 10.8.4 R RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS Safari 7 / iOS 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / OS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / OS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 9 / OS X 10.11 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_	OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4 R RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS Safari 7 / IOS 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / OS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS 8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / OS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 20 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Apple ATS 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_W	Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 7 / OS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / iOS 8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / iOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Apple ATS 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / OS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS 8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Apple ATS 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ECDH secp256r1 FS
Safari 8 / IOS 8.4 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 8 / IOS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 9 / IOS X 10.11 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Apple ATS 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / OS X 10.10 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS Safari 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 9 / OS X 10.11 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / IOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / OS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Apple ATS 9 / IOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 9 / OS X 10.11 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / OS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Apple ATS 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS eCDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS eCDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / iOS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Applie ATS 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Safari 10 / OS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Apple ATS 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS Apple ATS 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
	Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015 RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
	Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
<u>YandexBot Jan 2015</u> RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS	YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
# Not simulated clients (Protocol mismatch)	# Not simulated clients (Protoc	col mismatch)		E
IE 6 / XP No FS ¹ No SNI ² Protocol mismatch (not simulated)			in at aimsul-tN	

https://www.ssllabs.com/ssltest/analyze.html?d=www.flowtraders.com

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

Handshake Simulation

- (2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
- (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
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	Yes (with most browsers) ROBUST (more info)
ALPN	Yes http/1.1
NPN	No
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, secp521r1, brainpoolP512r1, brainpoolP384r1, secp384r1, brainpoolP256r1, secp256k1, sect571r1, sect571k1, sect409k1, sect409r1, sect283k1, sect283r1 (server preferred order)
SSL 2 handshake compatibility	Yes



HTTP Requests







Miscellaneous

Test date	Mon, 18 Feb 2019 16:39:42 UTC
Test duration	138.447 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	83.217.84.138.static.hosted.by.combell.com

SSL Report v1.32.16

Copyright © 2009-2019 Qualys, Inc. All Rights Reserved.

Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.