

# بررسی SSL دامنه rmt0.ir

تهیه شده توسط سامانه آنلاین بررسی SSL دامنه وب سایت SSL Labs.ir

تاریخ تهیه گزارش : چهارشنبه ۲۰ مرداد ۱۴۰۰ در ساعت ۱۰:۲۷  
بازدید: 0

گزارش بررسی تنظیمات SSL دامنه rmt0.ir

☆ امتیاز: ★★★★★

HSTS



آسیب پذیری



سازگاری مرورگرها



معتبر



ارتباط تنها در SSL



اطلاعات هدر دامنه

Date: Wed, 11 Aug 2021 06:05:37 GMT  
Server: Microsoft-IIS/7.5  
X-Frame-Options: SAMEORIGIN  
Request-Time: 2021-08-11 10:35:37  
Vary: Accept-Encoding  
Content-Encoding: gzip  
WAF-Mode: True  
X-XSS-Protection: 1; mode=block  
X-Permitted-Cross-Domain-Policies: master-only  
Web-Server: true  
Content-Length: 278  
Keep-Alive: timeout=15, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8

//:http

http://rmto.ir/ -&gt; 302 -&gt; https://rmto.ir/ -&gt; 200

//:https

https://rmto.ir/ -&gt; 200

همیشه از HTTPS استفاده کنید

تغییر همه درخواست ها با پروتکل "http" به "https".

(HTTP Strict Transport Security (HSTS)

اطلاعات بیشتر ?

ارائه نشده است HTTP Strict Transport Security (HSTS):

اطلاعات امضای دیجیتال صادر شده

## اطلاعات امضای دیجیتال شماره # 1

عنوان امضای دیجیتال : rmto.ir.

عنوان های جایگزین امضا (Alternative) , rmto.ir , rmto.ir

: (Names

شروع اعتبار از : چهارشنبه ۲۶ آذر ۱۳۹۹ در ساعت ۰۶:۵۶

پایان اعتبار تا : چهارشنبه ۲۴ آذر ۱۴۰۰ در ساعت ۰۶:۵۶ - اتمام در : 126 روز و 58 دقیقه و 39 ثانیه

صادر کننده مجوز : Certum Domain Validation CA SHA2

کشور صادر کننده مجوز : PL - لهستان

الگوریتم امضا : sha256 with RSA size: 2048 Bits

: Certificate Transparency (yes (certificate extension

: OCSP stapling (LOW - not offered

: OCSP URL http://dvcasha2.ocsp-certum.com

: CRL Distribution Points http://crl.certum.pl/dvcasha2.crl

Trust

Android iOS Java macOS Mozilla OPENJDK Windows

بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

نام هاست دامنه : rmt0.ir

انطباق دامنه با امضای دیجیتال : بلی

: Path Validation

Validation Result	Using Trust Store	Trust Store Version	#
ok	Android	r9_9.0.0	1
ok	iOS	macOS 10.14, watchOS 5, and tvOS 12 ,12	2
ok	Java	jdk-11.0.1	3
ok	macOS	macOS 10.14, watchOS 5, and tvOS 12 ,12	4
ok	Mozilla	2018-11-22	5
ok	OPENJDK	jdk-11.0.1	6
ok	Windows	2018-12-08	7

امضا های دیجیتال تایید شده :

\_\_\_ Sha1 پشتیبانی از امضای دیجیتال (Sha1 Signed Certificate). خیر

Successful Trust Store: Windows \_\_\_

\_\_\_ لیست امضا های تایید شده:

شماره 1 : =7cpbUae1hpieX8QleCZrDSGhFuszv2No+71XmIQXo5s

=Pin : 7cpbUae1hpieX8QleCZrDSGhFuszv2No+71XmIQXo5s

Finger print : 0af2bf3c736cd38481ed9aab7f471131d7731054

عنوان : commonName=.rmt0.ir

countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Domain Validation CA SHA2

سریال مجوز : 4.4442774003101E+37

شروع اعتبار از : 06:56:30 16-12-2020

پایان اعتبار تا : 06:56:30 15-12-2021

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 2 : =S4AbJNGvyS57nzJwv8sPMUML8VHSqH1vbiBftdPcErl

=Pin : S4AbJNGvyS57nzJwv8sPMUML8VHSqH1vbiBftdPcErl

Finger print : ff9ceb13c83f15b800e6eff987b2c72e01b4b320

عنوان : countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Domain Validation CA SHA2

countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Trusted Network CA

سریال مجوز : 5.1662424180299E+37

شروع اعتبار از : 12:00:00 11-09-2014

پایان اعتبار تا : 10:46:39 09-06-2027

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 3 : qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU =

=Pin : qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU

Finger print : 07e032e020b72c3f192f0628a2593a19a70f069e

countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Trusted Network CA : عنوان

countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Trusted Network : صادر کننده مجوز : CA

سریال مجوز : 279744

شروع اعتبار از : 12:07:37 22-10-2008

پایان اعتبار تا : 12:07:37 31-12-2029

الگوریتم امضا : sha1

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

: OCSF Stapling

خیر | پشتیبانی از OCSF : \_\_\_

خیر | OCSF Response : \_\_\_

خیر | Trusted By Mozilla \_\_\_ | \_\_\_

: CA Store

Type : DEFLATE - ندارد | Deflate Compression

(TLS Fallback Scsv) دارد | Downgrade Attacks Prevention

: Session Renegotiation

بلی | Secure Renegotiation \_\_\_

خیر | Insecure Client-Initiated \_\_\_

: Renegotiation

: Resumption Support

دارد | Resumption With TLS \_\_\_

: Tickets

ندارد | Resumption With Session \_\_\_

: IDs

ارائه نشده است Next Protocol Negotiation extension  
 : ((NPN  
 http/1.1 Application-Layer Protocol Negotiation  
 : ((ALPN

ارائه شده است : Personal Financial Specialist (PFS)

ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305 DHE-RSA-CHACHA20-POLY1305 DHE-RSA-AES256-CCM8 DHE-RSA-AES256-CCM DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA ECDHE-RSA-CAMELLIA256-SHA384 DHE-RSA-CAMELLIA256-SHA256 DHE-RSA-CAMELLIA256-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-CCM8 DHE-RSA-AES128-CCM DHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA ECDHE-RSA-CAMELLIA128-SHA256 DHE-RSA-CAMELLIA128-SHA256 DHE-RSA-SEED-SHA DHE-RSA-CAMELLIA128-SHA

: PFS Ciphers

prime256v1 secp384r1 secp521r1 : PFS ECDHE curves

RFC3526/Oakley Group 14 : DH Groups

Default protocol TLS1.2 : Protocol Negotiated

(ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256 : Cipher Negotiated

renegotiation info/#65281 EC point formats/#11 session ticket/#35 encrypt-then-mac/#22 extended master secret/#23 application layer protocol negotiation/#16 : TLS Extensions

(valid for 7200 seconds only ( < daily : TLS Session Ticket

yes : SSL SessionID Support

پشتیبانی می کند : Session Resumption Ticket

پشتیبانی نمی کند : Session Resumption ID

random : TLS Timestamp

-- : DNS CAA Record

(yes (certificate extension : Cert Transparency

( / ) Forbidden 403 : HTTP Status

ارائه نشده است (HTTP Strict Transport Security (HSTS

Microsoft-IIS/7.5 : Banner Server

No support for HTTP Public Key Pinning : (HTTP Public Key Pinning (HPKP

(at / (30x detected, better try target URL of 30x 0 : Cookie Count

no heartbeat extension , آسیب پذیر نیست , : Heartbleed

آسیب پذیر نیست : (Certified Coding Specialist (CCS

آسیب پذیر نیست : Ticketbleed

CVE-2016-9244 : CVE \_

CWE-200 : CVE \_

آسیب پذیر نیست : ROBOT

CVE-2017-17382 CVE-2017-17427 CVE-2017-17428 CVE-2017-13098 CVE-2017-1000385 CVE-2017-13099 CVE-2016-6883 CVE-2012-5081 CVE-2017-6168 : CVE \_

CWE-203 : CVE \_

آسیب پذیر نیست : Secure Renego

CVE-2009-3555 : CVE \_

CWE-310 : CVE \_

آسیب پذیر نیست : Secure Client Renego

CVE-2009-3555 : CVE \_

CWE-310 : CVE \_

آسیب پذیر نیست Compression Ratio Info-leak Made

CVE-2012-4929 : (Easy)CRIME

CWE-310 : CVE \_

ممکن است آسیب پذیر باشد , uses gzip HTTP compression - only supplied / tested : BREACH

CVE-2013-3587 : CVE \_

CWE-310 : CVE \_

پشتیبانی می کند : Fallback SCSV

آسیب پذیر نیست : POODLE SSL

CWE-310 : CVE \_

? اطلاعات بیشتر

? اطلاعات بیشتر

اطلاعات بیشتر ?	<p>آسیب پذیر نیست                  CVE-2016-2183 CVE-2016-6329                  CWE-327                  آسیب پذیر نیست</p>	<p>: SWEET32                  : CVE _                   : CVE _                   FREAK (Factoring RSA Export                  : (Keys</p>
اطلاعات بیشتر ?	<p>Make sure you don t use this certificate elsewhere with SSLv2 enabled services, see                  https://censys.io/ipv4?                  q=A45B06D03E260918FDE61AA8715409CFA4D27618D73DC017FCCB648975AA3B9A                  CVE-2016-0800 CVE-2016-0703                  CWE-310</p>	<p>DROWN (Decrypting RSA                  with Obsolete and                  : (Weakened eNcryption                  : CVE _                   : CVE _ </p>
اطلاعات بیشتر ?	<p>RFC3526/Oakley Group 14                  CVE-2015-4000                  CWE-310</p>	<p>: LOGJAM Common Primes                  : CVE _                   : CVE _ </p>
اطلاعات بیشتر ?	<p>,no DH EXPORT ciphers , آسیب پذیر نیست                  CVE-2015-4000                  CWE-310</p>	<p>: LOGJAM                  : CVE _                   : CVE _ </p>
اطلاعات بیشتر ?	<p>ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-CAMELLIA256-SHA                  ECDHE-RSA-AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-CAMELLIA128-SHA                  AES256-SHA CAMELLIA256-SHA AES128-SHA CAMELLIA128-SHA DHE-RSA-                  SEED-SHA SEED-SHA IDEA-CBC-SHA                  CVE-2011-3389                  CWE-20</p>	<p>: BEAST CBC TLS1                  : CVE _                   : CVE _ </p>
اطلاعات بیشتر ?	<p>but also supports higher protocols TLSv1.1 TLSv1.2 (likely – آسیب پذیر                  (mitigated                  همچنین از پروتکل های بالاتر TLSv1.1 TLSv1.2 پشتیبانی می کند                  CVE-2011-3389                  CWE-20                  ممکن است آسیب پذیر باشد, uses TLS CBC ciphers                  CVE-2013-0169                  CWE-310</p>	<p>: BEAST                  : CVE _                   : CVE _                   : LUCKY 13                  : CVE _                   : CVE _ </p>
اطلاعات بیشتر ?	<p>آسیب پذیر نیست                  CWE-310</p>	<p>: RC4                  : CVE _ </p>



پشتیبانی از این پروتکل : خیر

: Accepted Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Unexpected EOF	SSL_CK_RC4_128_WITH_MD5	1
خیر	TLS / Unexpected EOF	SSL_CK_RC4_128_EXPORT40_WITH_MD5	2
خیر	TLS / Unexpected EOF	SSL_CK_RC2_128_CBC_WITH_MD5	3
خیر	TLS / Unexpected EOF	SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	4
خیر	TLS / Unexpected EOF	SSL_CK_IDEA_128_CBC_WITH_MD5	5
خیر	TLS / Unexpected EOF	SSL_CK_DES_64_CBC_WITH_MD5	6
خیر	TLS / Unexpected EOF	SSL_CK_DES_192_EDE3_CBC_WITH_MD5	7

پشتیبانی از این پروتکل : خیر

: Accepted Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_SEED_CBC_SHA	1
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_RC4_128_SHA	2
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_RC4_128_MD5	3
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	4
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_NULL_SHA	5
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_NULL_MD5	6
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_IDEA_CBC_SHA	7
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_DES_CBC_SHA	8
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	10
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_256_GCM_SHA384	11
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_256_CBC_SHA256	12
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_AES_256_CBC_SHA	13
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_128_GCM_SHA256	14
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_128_CBC_SHA256	15
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_AES_128_CBC_SHA	16
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_3DES_EDE_CBC_SHA	17
خیر	TLS / Alert: handshake failure	TLS_RSA_EXPORT_WITH_RC4_40_MD5	18

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	20
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_RC4_128_SHA	21
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_NULL_SHA	22
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	23
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	24
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	25
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_RC4_128_SHA	26
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_NULL_SHA	27
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	28
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	29
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	30
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	31
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	32
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	33
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	34
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	35
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_NULL_SHA	36
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	37
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	38
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	39

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	40
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	41
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	42
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	43
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_RC4_128_SHA	44
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_NULL_SHA	45
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	46
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	47
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	48
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	49
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	50
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	51
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	52
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	53
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_NULL_SHA	54
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	55
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	56
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	57
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	58
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	59

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	60
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	61
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_SEED_CBC_SHA	62
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_RC4_128_MD5	63
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_DES_CBC_SHA	64
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	65
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	66
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_256_GCM_SHA384	67
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_256_CBC_SHA256	68
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA	69
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_128_GCM_SHA256	70
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_128_CBC_SHA256	71
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA	72
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	73
بلی	TLS / Alert: handshake failure	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	74
بلی	TLS / Alert: handshake failure	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	75
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_SEED_CBC_SHA	76
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_DES_CBC_SHA	77
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	78
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	79

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	80
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	81
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_AES_256_CBC_SHA	82
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	83
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	84
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_AES_128_CBC_SHA	85
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	86
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_SEED_CBC_SHA	87
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_DES_CBC_SHA	88
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	89
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	90
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	91
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	92
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_AES_256_CBC_SHA	93
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	94
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	95
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_AES_128_CBC_SHA	96
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	97
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_SEED_CBC_SHA	98
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_DES_CBC_SHA	99

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	100
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	101
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	102
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	103
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	104
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	105
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	106
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	107
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	108
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	109
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_SEED_CBC_SHA	110
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_DES_CBC_SHA	111
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	112
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	113
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	114
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	115
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	116
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	117
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	118
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	119

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	120
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	121



پشتیبانی از این پروتکل : بلی

## : Accepted Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	1
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	2
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	3
خیر	HTTP 200 OK	TLS_RSA_WITH_AES_256_CBC_SHA	4
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	5
خیر	HTTP 404 Not Found	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	6
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_SEED_CBC_SHA	7
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	8
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_AES_128_CBC_SHA	9
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_SEED_CBC_SHA	10
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	11
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_IDEA_CBC_SHA	12
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	13

## : Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	1

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_RC4_128_SHA	1
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_RC4_128_MD5	2
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	3
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_NULL_SHA	4

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_DES_CBC_SHA	6
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_256_GCM_SHA384	7
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_256_CBC_SHA256	8
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_128_GCM_SHA256	9
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_128_CBC_SHA256	10
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11
خیر	TLS / Alert: handshake failure	TLS_RSA_EXPORT_WITH_RC4_40_MD5	12
خیر	TLS / Alert: handshake failure	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	13
خیر	TLS / Alert: handshake failure	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	14
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_RC4_128_SHA	15
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_NULL_SHA	16
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	17
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	18
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	19
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_RC4_128_SHA	20
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_NULL_SHA	21
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	22
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	23
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	24
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	25

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	26
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	27
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	28
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	29
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_NULL_SHA	30
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	31
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	32
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	33
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	34
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	35
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	36
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	37
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_RC4_128_SHA	38
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_NULL_SHA	39
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	40
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	41
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	42
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	43
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	44
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	45

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_NULL_SHA	46
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	47
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	48
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	49
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	50
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	51
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	52
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	53
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_SEED_CBC_SHA	54
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_RC4_128_MD5	55
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_DES_CBC_SHA	56
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	57
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	58
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_256_GCM_SHA384	59
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_256_CBC_SHA256	60
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA	61
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_128_GCM_SHA256	62
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_128_CBC_SHA256	63
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA	64
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	65

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
بلی	TLS / Alert: handshake failure	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	66
بلی	TLS / Alert: handshake failure	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	67
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_SEED_CBC_SHA	68
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_DES_CBC_SHA	69
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	70
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	71
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	72
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	73
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_AES_256_CBC_SHA	74
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	75
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	76
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_AES_128_CBC_SHA	77
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	78
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_SEED_CBC_SHA	79
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_DES_CBC_SHA	80
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	81
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	82
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	83
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	84
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_AES_256_CBC_SHA	85

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	86
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	87
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_AES_128_CBC_SHA	88
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	89
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_DES_CBC_SHA	90
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	91
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	92
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	93
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	94
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	95
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	96
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_SEED_CBC_SHA	97
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_DES_CBC_SHA	98
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	99
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	100
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	101
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	102
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	103
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	104
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	105

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	106
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	107
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	108

پشتیبانی از این پروتکل : بلی

## : Accepted Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	1
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	2
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	3
خیر	HTTP 200 OK	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	4
خیر	HTTP 200 OK	TLS_RSA_WITH_AES_256_CBC_SHA	5
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	6
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	7
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_SEED_CBC_SHA	8
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	9
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	10
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_IDEA_CBC_SHA	11
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_SEED_CBC_SHA	12
خیر	HTTP 404 Not Found	TLS_RSA_WITH_AES_128_CBC_SHA	13

## : Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	1

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_RC4_128_SHA	1
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_RC4_128_MD5	2
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	3
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_NULL_SHA	4



## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_DES_CBC_SHA	6
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_256_GCM_SHA384	7
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_256_CBC_SHA256	8
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_128_GCM_SHA256	9
خیر	TLS / No ciphers available	TLS_RSA_WITH_AES_128_CBC_SHA256	10
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_3DES_EDE_CBC_SHA	11
خیر	TLS / Alert: handshake failure	TLS_RSA_EXPORT_WITH_RC4_40_MD5	12
خیر	TLS / Alert: handshake failure	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	13
خیر	TLS / Alert: handshake failure	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	14
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_RC4_128_SHA	15
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_NULL_SHA	16
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	17
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	18
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	19
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_RC4_128_SHA	20
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_NULL_SHA	21
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	22
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	23
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	24
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	25

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / No ciphers available	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	26
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	27
خیر	TLS / Alert: handshake failure	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	28
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	29
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_NULL_SHA	30
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	31
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	32
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	33
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	34
خیر	TLS / No ciphers available	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	35
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	36
خیر	TLS / Alert: handshake failure	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	37
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_RC4_128_SHA	38
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_NULL_SHA	39
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	40
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	41
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	42
خیر	TLS / No ciphers available	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	43
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	44
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	45

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_NULL_SHA	46
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	47
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	48
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	49
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	50
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	51
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	52
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	53
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_SEED_CBC_SHA	54
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_RC4_128_MD5	55
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_DES_CBC_SHA	56
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	57
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	58
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_256_GCM_SHA384	59
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_256_CBC_SHA256	60
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA	61
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_128_GCM_SHA256	62
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_AES_128_CBC_SHA256	63
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA	64
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	65

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
بلی	TLS / Alert: handshake failure	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	66
بلی	TLS / Alert: handshake failure	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	67
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_SEED_CBC_SHA	68
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_DES_CBC_SHA	69
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	70
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	71
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	72
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	73
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_AES_256_CBC_SHA	74
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	75
خیر	TLS / No ciphers available	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	76
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_AES_128_CBC_SHA	77
خیر	TLS / Alert: handshake failure	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	78
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_SEED_CBC_SHA	79
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_DES_CBC_SHA	80
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	81
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	82
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	83
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	84
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_AES_256_CBC_SHA	85

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	86
خیر	TLS / No ciphers available	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	87
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_AES_128_CBC_SHA	88
خیر	TLS / Alert: handshake failure	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	89
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_DES_CBC_SHA	90
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	91
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	92
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	93
خیر	TLS / No ciphers available	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	94
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	95
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	96
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_SEED_CBC_SHA	97
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_DES_CBC_SHA	98
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	99
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	100
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	101
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	102
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	103
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	104
خیر	TLS / No ciphers available	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	105

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	106
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	107
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	108

## : Accepted Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	RSA_WITH_AES_256_CCM_8	1
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	2
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	3
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	4
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	5
خیر	HTTP 200 OK	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	6
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	7
خیر	HTTP 200 OK	RSA_WITH_AES_256_CCM	8
خیر	HTTP 404 Not Found	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	10
خیر	HTTP 404 Not Found	TLS_RSA_WITH_AES_256_CBC_SHA256	11
خیر	HTTP 404 Not Found	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	12
خیر	HTTP 403 Forbidden	DHE_RSA_WITH_AES_256_CCM_8	13
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	14
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	15
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	16
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	17
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_AES_256_GCM_SHA384	18
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_AES_256_CCM	19

## : Accepted Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_AES_256_CBC_SHA	20
خیر	HTTP 200 OK	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	21
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	22
خیر	HTTP 200 OK	RSA_WITH_AES_128_CCM_8	23
خیر	HTTP 200 OK	RSA_WITH_AES_128_CCM	24
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	25
خیر	HTTP 200 OK	DHE_RSA_WITH_AES_128_CCM	26
خیر	HTTP 404 Not Found	TLS_RSA_WITH_SEED_CBC_SHA	27
خیر	HTTP 403 Forbidden	DHE_RSA_WITH_AES_128_CCM_8	28
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	29
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	30
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	31
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	32
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_AES_128_CBC_SHA	33
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_AES_128_CBC_SHA256	34
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	35
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_AES_128_GCM_SHA256	36
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	37
خیر	HTTP 403 Forbidden	TLS_DHE_RSA_WITH_SEED_CBC_SHA	38
خیر	HTTP 403 Forbidden	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	39



## : Accepted Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	40

## : Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 403 Forbidden	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	1

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_RC4_128_SHA	1
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_RC4_128_MD5	2
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_NULL_SHA256	3
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_NULL_SHA	4
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_NULL_MD5	5
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_IDEA_CBC_SHA	6
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_3DES_EDE_CBC_SHA	7
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_RC4_128_SHA	8
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_NULL_SHA	9
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	10
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	11
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	12
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_RC4_128_SHA	13
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_NULL_SHA	14
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	15
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	16
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_NULL_SHA	17

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	19
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	20
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	21
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	22
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	23
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	24
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	25
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	26
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	27
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_SEED_CBC_SHA	28
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_RC4_128_MD5	29
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	30
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	31
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	32
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	33
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_GCM_SHA384	34
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA256	35
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA	36
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_GCM_SHA256	37
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA256	38

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA	39
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	40
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	41
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_SEED_CBC_SHA	42
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	43
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	44
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	45
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	46
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	47
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	48
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	49
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	50
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	51
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	52
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	53
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_256_CCM_8	54
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_256_CCM	55
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_128_CCM_8	56
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_128_CCM	57
خیر	TLS / Alert: handshake failure	ECDHE-ECDSA-ARIA256-GCM-SHA384	58

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	ECDHE-ECDSA-ARIA128-GCM-SHA256	59
خیر	TLS / Alert: handshake failure	ECDHE-ARIA256-GCM-SHA384	60
خیر	TLS / Alert: handshake failure	ECDHE-ARIA128-GCM-SHA256	61
خیر	TLS / Alert: handshake failure	DHE-RSA-ARIA256-GCM-SHA384	62
خیر	TLS / Alert: handshake failure	DHE-RSA-ARIA128-GCM-SHA256	63
خیر	TLS / Alert: handshake failure	DHE-DSS-ARIA256-GCM-SHA384	64
خیر	TLS / Alert: handshake failure	DHE-DSS-ARIA128-GCM-SHA256	65
خیر	TLS / Alert: handshake failure	ARIA256-GCM-SHA384	66
خیر	TLS / Alert: handshake failure	ARIA128-GCM-SHA256	67

: Handshake Simulation

Cipher	Type	Name	#
TLS_RSA_WITH_AES_128_CBC_SHA	tlsv1	(Android(2.3.7	1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(Android(4.0.4	2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(Android(4.1.1	3
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(Android(4.2.2	4
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(Android(4.3	5
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(Android(4.4.2	6
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(Android(5.0.0	7
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	(Android(6.0	8
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	tlsv1_2	(Android(7.0	9
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(Baidu(Jan 2015	10
TLS_RSA_WITH_AES_128_CBC_SHA	tlsv1	(BingBot(Dec 2013	11
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(BingPreview(Dec 2013	12
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(BingPreview(Jun 2014	13
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(BingPreview(Jan 2015	14
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Chrome(27) - Win 7	15
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Chrome(28) - Win 7	16
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Chrome(29) - Win 7	17
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Chrome(30) - Win 7	18
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(31) - Win 7	19

: Handshake Simulation

Cipher	Type	Name	#
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(32) - Win 7	20
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(33) - Win 7	21
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(34) - OS X	22
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(35) - Win 7	23
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(36) - Win 7	24
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(37) - OS X	25
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(39) - OS X	26
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(40) - OS X	27
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(42) - OS X	28
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(43) - OS X	29
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(45) - OS X	30
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(47) - OS X	31
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(48) - OS X	32
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(49) - Win 7	33
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(49) - XP SP3	34
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(50) - Win 7	35
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(51) - Win 7	36
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Chrome(57) - Win 7	37
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Firefox(21) - Win 7	38
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Firefox(10.0.12 ESR) - Win 7	39

: Handshake Simulation

Cipher	Type	Name	#
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Firefox(17.0.7 ESR) - Win 7	40
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Firefox(24.2.0 ESR) - Win 7	41
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(31.3.0 ESR) - Win 7	42
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	tlsv1	Firefox(21) - Fedora 19	43
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Firefox(22) - Win 7	44
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Firefox(24) - Win 7	45
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Firefox(26) - Win 8	46
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(27) - Win 8	47
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(29) - OS X	48
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(30) - OS X	49
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(31) - OS X	50
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(32) - OS X	51
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(34) - OS X	52
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(35) - OS X	53
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(37) - OS X	54
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(39) - OS X	55
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(41) - OS X	56
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(42) - OS X	57
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(44) - OS X	58
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(45) - Win 7	59

: Handshake Simulation

Cipher	Type	Name	#
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(46) - Win 7	60
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(47) - Win 7	61
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(49) - XP SP3	62
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(49) - Win 7	63
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	Firefox(53) - Win 7	64
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	tlsv1	(Googlebot(Oct 2013	65
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	tlsv1	(Googlebot(Jun 2014	66
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	(Googlebot(Feb 2015	67
		IE(6) - XP	68
		IE(6) - XP	69
TLS_RSA_WITH_AES_128_CBC_SHA	tlsv1	IE(7) - Vista	70
		IE(8) - XP	71
		IE(8) - XP	72
TLS_RSA_WITH_AES_128_CBC_SHA	tlsv1	IE(8) - Win 7	73
TLS_RSA_WITH_AES_128_CBC_SHA	tlsv1	IE(9) - Win 7	74
TLS_RSA_WITH_AES_128_CBC_SHA	tlsv1	IE(8-10) - Win 7	75
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	IE(8-10) - Win 7	76
TLS_RSA_WITH_AES_128_CBC_SHA256	tlsv1_2	IE(11) - Win 7	77
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win 7	78
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win 7	79



## : Handshake Simulation

Cipher	Type	Name	#
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win 7	80
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win 7	81
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 10 Preview	82
TLS_RSA_WITH_AES_128_CBC_SHA256	tlsv1_2	IE(11) - Win 8.1	83
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win 8.1	84
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win 8.1	85
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win 8.1	86
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win 8.1	87
TLS_RSA_WITH_AES_128_CBC_SHA	tlsv1	IE(10) - Win Phone 8.0	88
TLS_RSA_WITH_AES_128_CBC_SHA256	tlsv1_2	IE(11) - Win Phone 8.1	89
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	IE(11) - Win Phone 8.1 Update	90
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 10	91
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 10	92
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Edge(12) - Win 10	93
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Edge(13) - Win 10	94
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Edge(13) - Win 10	95
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Edge(13) - Win Phone 10	96
TLS_RSA_WITH_AES_128_CBC_SHA	tlsv1	(Java(6u45	97
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	tlsv1	(Java(7u25	98
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	tlsv1_2	(Java(8b132	99

: Handshake Simulation

Cipher	Type	Name	#
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	tlsv1_2	(Java(8u31	100
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(OpenSSL(0.9.8y	101
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(OpenSSL(1.0.1h	102
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(OpenSSL(1.0.1l	103
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(OpenSSL(1.0.2e	104
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	tlsv1_2	Opera(12.15) - Win 7	105
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Opera(15) - Win 7	106
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Opera(16) - Win 7	107
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Opera(17) - Win 7	108
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	Safari(5) - iOS 5.1.1	109
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	tlsv1	Safari(5.1.9) - OS X 10.6.8	110
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	Safari(6) - iOS 6.0.1	111
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Safari(6.0.4) - OS X 10.8.4	112
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	Safari(7) - iOS 7.1	113
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	Safari(8) - iOS 8.0 Beta	114
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	Safari(7) - OS X 10.9	115
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	Safari(8) - iOS 8.4	116
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	Safari(8) - OS X 10.10	117
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Safari(9) - iOS 9	118
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Safari(9) - OS X 10.11	119

: Handshake Simulation

Cipher	Type	Name	#
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Safari(10) - iOS 10	120
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Safari(10) - OS X 10.12	121
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	Apple ATS(9) - iOS 9	122
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	Tor(17.0.9) - Win 7	123
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(Yahoo Slurp(Oct 2013	124
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(Yahoo Slurp(Jun 2014	125
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(Yahoo Slurp(Jan 2015	126
		(YandexBot(3.0	127
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	tlsv1	(YandexBot(May 2014	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(YandexBot(Sep 2014	129
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(YandexBot(Jan 2015	130

