

# بررسی SSL دامنه partosanatco.ir

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

تاریخ تهیه گزارش : چهارشنبه ۹ تیر ۱۴۰۰ در ساعت ۱۴:۱۸  
بازدید: 0

گزارش بررسی تنظیمات SSL دامنه partosanatco.ir

☆ امتیاز: ★★★★★

HSTS



آسیب پذیری



سازگاری مرورگرها



معتبر



ارتباط تنها در SSL



اطلاعات هدر دامنه

Content-Type: text/html  
Content-Encoding: gzip  
Last-Modified: Sun, 24 Jan 2021 11:35:14 GMT  
Accept-Ranges: bytes  
ETag: "30cd93fb44f2d61:0"  
Vary: Accept-Encoding  
Server: -  
Strict-Transport-Security: max-age=31536000; includeSubDomains  
Date: Wed, 30 Jun 2021 09:48:05 GMT  
Content-Length: 400

//:http

http://partosanatco.ir/ -&gt; 301 -&gt; https://partosanatco.ir/ -&gt; 200

//:https

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

همیشه از HTTPS استفاده کنید

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

(HTTP Strict Transport Security (HSTS

اطلاعات بیشتر ?

HTTP Strict Transport Security  
: (TIME (HSTS  
includes subdomains HTTP Strict Transport Security  
: (SubDomains (HSTS  
domain is NOT marked for preloading HTTP Strict Transport Security  
: (Preload (HSTS

اطلاعات امضای دیجیتال صادر شده

## اطلاعات امضای دیجیتال شماره 1 #

عنوان امضای دیجیتال : partosanatco.ir.

عنوان های جایگزین امضا (Alternative) , ,

: (Names

شروع اعتبار از :

چهارشنبه ۰۹ تیر ۱۴۰۰ در ساعت ۰۸:۳۵

پایان اعتبار تا :

سه شنبه ۰۶ مهر ۱۴۰۰ در ساعت ۰۸:۳۵ - اتمام در : 89 روز و 21 ساعت و 47 دقیقه و 17 ثانیه

صادر کننده مجوز :

R3

کشور صادر کننده مجوز :

US - ایالات متحده (آمریکا)

الگوریتم امضا :

sha256 with RSA size: 4096 Bits

: Certificate Transparency

(yes (certificate extension

: OCSP stapling

OK - offered

: OCSP URL

http://r3.o.lencr.org

: CRL Distribution Points

--

Trust

Android iOS Java macOS Mozilla OPENJDK Windows

بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

نام هاست دامنه : partosanatco.ir

انطباق دامنه با امضای دیجیتال : خیر

: 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 : syOgaykoTjshGaBRwiXFj6clOBlcJV2I5jQBV5ikF8E =

=Pin : syOgaykoTjshGaBRwiXFj6clOBlcJV2I5jQBV5ikF8E

Finger print : 0099775c9f62a0408e1b295d8ede363169d72c31

عنوان : commonName=.partosanatco.ir

صادر کننده مجوز : countryName=US, organizationName=Lets Encrypt, commonName=R3

سریال مجوز : 3.3806612823965E+41

شروع اعتبار از : 08:35:29 30-06-2021

پایان اعتبار تا : 08:35:28 28-09-2021

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 4096

شماره 2 : =jQJTblh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0

=Pin : jQJTblh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0

Finger print : 48504e974c0dac5b5cd476c8202274b24c8c7172

عنوان : countryName=US, organizationName=Lets Encrypt, commonName=R3

صادر کننده مجوز : organizationName=Digital Signature Trust Co., commonName=DST Root CA X3

سریال مجوز : 8.5078157426497E+37

شروع اعتبار از : 19:21:40 07-10-2020

پایان اعتبار تا : 19:21:40 29-09-2021

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 3 : =Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys

=Pin : Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys

**Finger print** : dac9024f54d8f6df94935fb1732638ca6ad77c13

organizationName=Digital Signature Trust Co., commonName=DST Root CA X3 : عنوان

organizationName=Digital Signature Trust Co., commonName=DST Root CA X3 : صادر کننده مجوز :

سریال مجوز : 9.129973557534E+37

شروع اعتبار از : 21:12:19 30-09-2000

پایان اعتبار تا : 14:01:15 30-09-2021

الگوریتم امضا : sha1

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

: OCSF Stapling

بلی : پشتیبانی از OCSF \_\_\_

بلی : OCSF Response \_\_\_

بلی Trusted By Mozilla \_\_\_

: CA Store

C = US, O = Lets Encrypt, CN = R3 : Responder ID \_\_\_

: Response Status \_\_\_

Jun 30 09:35:00 2021 GMT : Produced At \_\_\_

Type : DEFLATE - ندارد : Deflate Compression

(TLS Fallback Scsv) دارد : Downgrade Attacks Prevention

: Session Renegotiation

خیر : Secure Renegotiation \_\_\_

خیر Insecure Client-Initiated \_\_\_

: Renegotiation

: Resumption Support

ندارد Resumption With TLS \_\_\_

: Tickets

دارد Resumption With Session \_\_\_

: IDs

5 : تعداد کل تست های انجام شده : \_\_\_

5 : تست های موفقیت آمیز : \_\_\_

0 : تست های بدون پاسخ : \_\_\_

0 : تعداد خطا ها : \_\_\_

	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 DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-			: PFS Ciphers
AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 DHE-RSA-AES128-GCM-SHA256			: PFS ECDHE curves
prime256v1 secp384r1 X25519			: DH Groups
ffdhe2048			: Protocol Negotiated
Default protocol TLS1.2			: Cipher Negotiated
(ECDHE-RSA-AES256-GCM-SHA384, 384 bit ECDH (P-384			: TLS Extensions
status request/#5 renegotiation info/#65281 application layer protocol negotiation/#16 extended master secret/#23			: TLS Session Ticket
No lifetime advertised			: SSL SessionID Support
yes			: Session Resumption Ticket
پشتیبانی نمی کند			: Session Resumption ID
پشتیبانی نمی کند			: TLS Timestamp
off by -1 seconds from your localtime			: DNS CAA Record
--			: Cert Transparency
(yes (certificate extension			: HTTP Status
( / ) OK 200			HTTP Strict Transport Security TIME
days (=31536000 seconds) > 15465600 seconds 365			: ((HSTS
			HTTP Strict Transport Security
includes subdomains			: (SubDomains (HSTS
			HTTP Strict Transport Security
domain is NOT marked for preloading			: (Preload (HSTS
-			: Banner Server
No support for HTTP Public Key Pinning			: (HTTP Public Key Pinning (HPKP
/ at 0			: Cookie Count
no heartbeat extension , آسیب پذیر نیست			: Heartbleed
آسیب پذیر نیست			: (Certified Coding Specialist (CCS
no session ticket extension			: 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-			: 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
			: (Easy(CRIME
CVE-2012-4929			: CVE _
CWE-310			: CVE _
uses gzip HTTP compression - only supplied / tested , ممکن است آسیب پذیر باشد			: BREACH
CVE-2013-3587			: CVE _
CWE-310			: CVE _

[اطلاعات بیشتر](#)

اطلاعات بیشتر ?

no protocol below TLS 1.2 offered

آسیب پذیر نیست

CWE-310

آسیب پذیر نیست

CVE-2016-2183 CVE-2016-6329

CWE-327

آسیب پذیر نیست

: Fallback SCSV

: POODLE SSL

: CVE \_|

: SWEET32

: CVE \_|

: CVE \_|

FREAK (Factoring RSA Export

: (Keys

اطلاعات بیشتر ?

اطلاعات بیشتر ?

Make sure you don t use this certificate elsewhere with SSLv2 enabled services, see  
https://censys.io/ipv4?

q=5DDC8A0C94C35B2DEE1F729A09D983DEBD64E72EBA02E744156E8F95B23DBE87

CVE-2016-0800 CVE-2016-0703

CWE-310

RFC7919/ffdhe2048

CVE-2015-4000

CWE-310

,no DH EXPORT ciphers ,آسیب پذیر نیست

CVE-2015-4000

CWE-310

no SSL3 or TLS1 ,آسیب پذیر نیست

CVE-2011-3389

CWE-20

uses TLS CBC ciphers ,ممکن است آسیب پذیر باشد

CVE-2013-0169

CWE-310

آسیب پذیر نیست

CWE-310

DROWN (Decrypting RSA  
with Obsolete and

: (Weakened eNcryption

: CVE \_|

: CVE \_|

: LOGJAM Common Primes

: CVE \_|

: CVE \_|

: LOGJAM

: CVE \_|

: CVE \_|

: BEAST

: CVE \_|

: CVE \_|

: LUCKY 13

: CVE \_|

: CVE \_|

: RC4

: CVE \_|

اطلاعات بیشتر ?



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	TCP / Received RST	SSL_CK_RC4_128_WITH_MD5	1
خیر	TCP / Received RST	SSL_CK_RC4_128_EXPORT40_WITH_MD5	2
خیر	TCP / Received RST	SSL_CK_RC2_128_CBC_WITH_MD5	3
خیر	TCP / Received RST	SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	4
خیر	TCP / Received RST	SSL_CK_IDEA_128_CBC_WITH_MD5	5
خیر	TCP / Received RST	SSL_CK_DES_64_CBC_WITH_MD5	6
خیر	TCP / Received RST	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	TCP / Received RST	TLS_RSA_WITH_SEED_CBC_SHA	1
خیر	TCP / Received RST	TLS_RSA_WITH_RC4_128_SHA	2
خیر	TCP / Received RST	TLS_RSA_WITH_RC4_128_MD5	3
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	4
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_SHA	5
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_MD5	6
خیر	TCP / Received RST	TLS_RSA_WITH_IDEA_CBC_SHA	7
خیر	TCP / Received RST	TLS_RSA_WITH_DES_CBC_SHA	8
خیر	TCP / Received RST	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_RSA_WITH_AES_128_CBC_SHA	16
خیر	TCP / Received RST	TLS_RSA_WITH_3DES_EDE_CBC_SHA	17
خیر	TCP / Received RST	TLS_RSA_EXPORT_WITH_RC4_40_MD5	18

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	20
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_RC4_128_SHA	21
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_NULL_SHA	22
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	23
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	24
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	25
خیر	TCP / Received RST	TLS_ECDH_RSA_WITH_RC4_128_SHA	26
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	33
خیر	TCP / Received RST	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	34
خیر	TCP / Received RST	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	35
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	42
خیر	TCP / Received RST	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	43
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_RC4_128_SHA	44
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	51
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	52
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	53
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	60
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	61
بلی	TCP / Received RST	TLS_DH_anon_WITH_SEED_CBC_SHA	62
بلی	TCP / Received RST	TLS_DH_anon_WITH_RC4_128_MD5	63
بلی	TCP / Received RST	TLS_DH_anon_WITH_DES_CBC_SHA	64
بلی	TCP / Received RST	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	65
بلی	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DH_anon_WITH_AES_128_CBC_SHA	72
بلی	TCP / Received RST	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	73
بلی	TCP / Received RST	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	74
بلی	TCP / Received RST	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	75
خیر	TCP / Received RST	TLS_DH_RSA_WITH_SEED_CBC_SHA	76
خیر	TCP / Received RST	TLS_DH_RSA_WITH_DES_CBC_SHA	77
خیر	TCP / Received RST	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	78
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DH_RSA_WITH_AES_128_CBC_SHA	85
خیر	TCP / Received RST	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	86
خیر	TCP / Received RST	TLS_DH_DSS_WITH_SEED_CBC_SHA	87
خیر	TCP / Received RST	TLS_DH_DSS_WITH_DES_CBC_SHA	88
خیر	TCP / Received RST	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	89
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DH_DSS_WITH_AES_128_CBC_SHA	96
خیر	TCP / Received RST	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	97
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_SEED_CBC_SHA	98
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_DES_CBC_SHA	99

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	100
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	107
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	108
خیر	TCP / Received RST	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	109
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_SEED_CBC_SHA	110
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_DES_CBC_SHA	111
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	112
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	119

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	120
خیر	TCP / Received RST	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	121



— پشتیبانی از این پروتکل : خیر

: Accepted Cipher Suites

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

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر			1

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_RSA_WITH_SEED_CBC_SHA	1
خیر	TCP / Received RST	TLS_RSA_WITH_RC4_128_SHA	2
خیر	TCP / Received RST	TLS_RSA_WITH_RC4_128_MD5	3
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	4
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_SHA	5
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_MD5	6
خیر	TCP / Received RST	TLS_RSA_WITH_IDEA_CBC_SHA	7
خیر	TCP / Received RST	TLS_RSA_WITH_DES_CBC_SHA	8
خیر	TCP / Received RST	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_RSA_WITH_AES_128_CBC_SHA	16
خیر	TCP / Received RST	TLS_RSA_WITH_3DES_EDE_CBC_SHA	17

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	19
خیر	TCP / Received RST	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	20
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_RC4_128_SHA	21
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_NULL_SHA	22
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	23
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	24
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	25
خیر	TCP / Received RST	TLS_ECDH_RSA_WITH_RC4_128_SHA	26
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	33
خیر	TCP / Received RST	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	34
خیر	TCP / Received RST	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	35
خیر	TCP / Received RST	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

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	39
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	TCP / Received RST	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	42
خیر	TCP / Received RST	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	43
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_RC4_128_SHA	44
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	51
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	52
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	53
خیر	TCP / Received RST	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	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	57
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	58

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	59
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	60
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	61
بلی	TCP / Received RST	TLS_DH_anon_WITH_SEED_CBC_SHA	62
بلی	TCP / Received RST	TLS_DH_anon_WITH_RC4_128_MD5	63
بلی	TCP / Received RST	TLS_DH_anon_WITH_DES_CBC_SHA	64
بلی	TCP / Received RST	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	65
بلی	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DH_anon_WITH_AES_128_CBC_SHA	72
بلی	TCP / Received RST	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	73
بلی	TCP / Received RST	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	74
بلی	TCP / Received RST	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	75
خیر	TCP / Received RST	TLS_DH_RSA_WITH_SEED_CBC_SHA	76
خیر	TCP / Received RST	TLS_DH_RSA_WITH_DES_CBC_SHA	77
خیر	TCP / Received RST	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	78

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	79
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	TCP / Received RST	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	TCP / Received RST	TLS_DH_RSA_WITH_AES_128_CBC_SHA	85
خیر	TCP / Received RST	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	86
خیر	TCP / Received RST	TLS_DH_DSS_WITH_SEED_CBC_SHA	87
خیر	TCP / Received RST	TLS_DH_DSS_WITH_DES_CBC_SHA	88
خیر	TCP / Received RST	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	89
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DH_DSS_WITH_AES_128_CBC_SHA	96
خیر	TCP / Received RST	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	97
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_SEED_CBC_SHA	98

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_DES_CBC_SHA	99
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	100
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	107
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	108
خیر	TCP / Received RST	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	109
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_SEED_CBC_SHA	110
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_DES_CBC_SHA	111
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	112
خیر	TCP / Received RST	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	TCP / Received RST	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

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	119
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	120
خیر	TCP / Received RST	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	121

پشتیبانی از این پروتکل : خیر

: Accepted Cipher Suites

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

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر			1

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_RSA_WITH_SEED_CBC_SHA	1
خیر	TCP / Received RST	TLS_RSA_WITH_RC4_128_SHA	2
خیر	TCP / Received RST	TLS_RSA_WITH_RC4_128_MD5	3
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	4
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_SHA	5
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_MD5	6
خیر	TCP / Received RST	TLS_RSA_WITH_IDEA_CBC_SHA	7
خیر	TCP / Received RST	TLS_RSA_WITH_DES_CBC_SHA	8
خیر	TCP / Received RST	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_RSA_WITH_AES_128_CBC_SHA	16
خیر	TCP / Received RST	TLS_RSA_WITH_3DES_EDE_CBC_SHA	17



## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	19
خیر	TCP / Received RST	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	20
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_RC4_128_SHA	21
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_NULL_SHA	22
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	23
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	24
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	25
خیر	TCP / Received RST	TLS_ECDH_RSA_WITH_RC4_128_SHA	26
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	33
خیر	TCP / Received RST	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	34
خیر	TCP / Received RST	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	35
خیر	TCP / Received RST	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

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	39
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	TCP / Received RST	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	42
خیر	TCP / Received RST	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	43
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_RC4_128_SHA	44
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	51
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	52
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	53
خیر	TCP / Received RST	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	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	57
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	58

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / No ciphers available	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	59
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	60
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	61
بلی	TCP / Received RST	TLS_DH_anon_WITH_SEED_CBC_SHA	62
بلی	TCP / Received RST	TLS_DH_anon_WITH_RC4_128_MD5	63
بلی	TCP / Received RST	TLS_DH_anon_WITH_DES_CBC_SHA	64
بلی	TCP / Received RST	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	65
بلی	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DH_anon_WITH_AES_128_CBC_SHA	72
بلی	TCP / Received RST	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	73
بلی	TCP / Received RST	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	74
بلی	TCP / Received RST	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	75
خیر	TCP / Received RST	TLS_DH_RSA_WITH_SEED_CBC_SHA	76
خیر	TCP / Received RST	TLS_DH_RSA_WITH_DES_CBC_SHA	77
خیر	TCP / Received RST	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	78

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	79
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	TCP / Received RST	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	TCP / Received RST	TLS_DH_RSA_WITH_AES_128_CBC_SHA	85
خیر	TCP / Received RST	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	86
خیر	TCP / Received RST	TLS_DH_DSS_WITH_SEED_CBC_SHA	87
خیر	TCP / Received RST	TLS_DH_DSS_WITH_DES_CBC_SHA	88
خیر	TCP / Received RST	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	89
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DH_DSS_WITH_AES_128_CBC_SHA	96
خیر	TCP / Received RST	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	97
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_SEED_CBC_SHA	98

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_DES_CBC_SHA	99
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	100
خیر	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	107
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	108
خیر	TCP / Received RST	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	109
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_SEED_CBC_SHA	110
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_DES_CBC_SHA	111
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	112
خیر	TCP / Received RST	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	TCP / Received RST	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

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	119
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	120
خیر	TCP / Received RST	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_RSA_WITH_AES_256_CBC_SHA256	1
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	2
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	3
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	4
خیر	HTTP 200 OK	TLS_RSA_WITH_AES_256_GCM_SHA384	5
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	6
خیر	HTTP 200 OK	TLS_RSA_WITH_AES_128_CBC_SHA256	7
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	8
خیر	HTTP 200 OK	TLS_RSA_WITH_AES_128_GCM_SHA256	9
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	10

## Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	1

## Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_RSA_WITH_SEED_CBC_SHA	1
خیر	TCP / Received RST	TLS_RSA_WITH_RC4_128_SHA	2
خیر	TCP / Received RST	TLS_RSA_WITH_RC4_128_MD5	3
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_SHA256	4
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_SHA	5
خیر	TCP / Received RST	TLS_RSA_WITH_NULL_MD5	6
خیر	TCP / Received RST	TLS_RSA_WITH_IDEA_CBC_SHA	7

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	TCP / Received RST	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	10
خیر	TCP / Received RST	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	11
خیر	TCP / Received RST	TLS_RSA_WITH_AES_256_CBC_SHA	12
خیر	TCP / Received RST	TLS_RSA_WITH_AES_128_CBC_SHA	13
خیر	TCP / Received RST	TLS_RSA_WITH_3DES_EDE_CBC_SHA	14
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_RC4_128_SHA	15
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_NULL_SHA	16
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	17
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	18
بلی	TCP / Received RST	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	19
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_RC4_128_SHA	20
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_NULL_SHA	21
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	22
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	23
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	24
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	25
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	26
خیر	TCP / Received RST	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	27
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	28



## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_NULL_SHA	29
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	30
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	31
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	32
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	33
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	34
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	35
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	36
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	37
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	38
خیر	TCP / Received RST	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	39
بلی	TCP / Received RST	TLS_DH_anon_WITH_SEED_CBC_SHA	40
بلی	TCP / Received RST	TLS_DH_anon_WITH_RC4_128_MD5	41
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	42
بلی	TCP / Received RST	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	43
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	44
بلی	TCP / Received RST	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	45
بلی	TCP / Received RST	TLS_DH_anon_WITH_AES_256_GCM_SHA384	46
بلی	TCP / Received RST	TLS_DH_anon_WITH_AES_256_CBC_SHA256	47
بلی	TCP / Received RST	TLS_DH_anon_WITH_AES_256_CBC_SHA	48

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
بلی	TCP / Received RST	TLS_DH_anon_WITH_AES_128_GCM_SHA256	49
بلی	TCP / Received RST	TLS_DH_anon_WITH_AES_128_CBC_SHA256	50
بلی	TCP / Received RST	TLS_DH_anon_WITH_AES_128_CBC_SHA	51
بلی	TCP / Received RST	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	52
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_SEED_CBC_SHA	53
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	54
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	55
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	56
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	57
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	58
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_AES_256_CCM	59
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	60
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	61
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	62
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	63
خیر	TCP / Received RST	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	64
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_SEED_CBC_SHA	65
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	66
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	67
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	68

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	69
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	70
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	71
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	72
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	73
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	74
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	75
خیر	TCP / Received RST	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	76
خیر	TCP / Received RST	RSA_WITH_AES_256_CCM_8	77
خیر	TCP / Received RST	RSA_WITH_AES_256_CCM	78
خیر	TCP / Received RST	RSA_WITH_AES_128_CCM_8	79
خیر	TCP / Received RST	RSA_WITH_AES_128_CCM	80
خیر	TCP / Received RST	ECDHE_ECDSA_WITH_AES_256_CCM_8	81
خیر	TCP / Received RST	ECDHE_ECDSA_WITH_AES_256_CCM	82
خیر	TCP / Received RST	ECDHE_ECDSA_WITH_AES_128_CCM_8	83
خیر	TCP / Received RST	ECDHE_ECDSA_WITH_AES_128_CCM	84
خیر	TCP / Received RST	ECDHE-ECDSA-ARIA256-GCM-SHA384	85
خیر	TCP / Received RST	ECDHE-ECDSA-ARIA128-GCM-SHA256	86
خیر	TCP / Received RST	ECDHE-ARIA256-GCM-SHA384	87
خیر	TCP / Received RST	ECDHE-ARIA128-GCM-SHA256	88

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TCP / Received RST	DHE_RSA_WITH_AES_256_CCM_8	89
خیر	TCP / Received RST	DHE_RSA_WITH_AES_128_CCM_8	90
خیر	TCP / Received RST	DHE_RSA_WITH_AES_128_CCM	91
خیر	TCP / Received RST	DHE-RSA-ARIA256-GCM-SHA384	92
خیر	TCP / Received RST	DHE-RSA-ARIA128-GCM-SHA256	93
خیر	TCP / Received RST	DHE-DSS-ARIA256-GCM-SHA384	94
خیر	TCP / Received RST	DHE-DSS-ARIA128-GCM-SHA256	95
خیر	TCP / Received RST	ARIA256-GCM-SHA384	96
خیر	TCP / Received RST	ARIA128-GCM-SHA256	97

## : Handshake Simulation

Cipher	Type	Name	#
		(Android(2.3.7	1
		(Android(4.0.4	2
		(Android(4.1.1	3
		(Android(4.2.2	4
		(Android(4.3	5
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(Android(4.4.2	6
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	(Android(5.0.0	7
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	(Android(6.0	8
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	tlsv1_2	(Android(7.0	9
		(Baidu(Jan 2015	10
		(BingBot(Dec 2013	11
		(BingPreview(Dec 2013	12
		(BingPreview(Jun 2014	13
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	(BingPreview(Jan 2015	14
		Chrome(27) - Win 7	15
		Chrome(28) - Win 7	16
TLS_RSA_WITH_AES_256_CBC_SHA256	tlsv1_2	Chrome(29) - Win 7	17
TLS_RSA_WITH_AES_256_CBC_SHA256	tlsv1_2	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
		Firefox(21) - Win 7	38
		Firefox(10.0.12 ESR) - Win 7	39

## : Handshake Simulation

Cipher	Type	Name	#
		Firefox(17.0.7 ESR) - Win 7	40
		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
		Firefox(21) - Fedora 19	43
		Firefox(22) - Win 7	44
		Firefox(24) - Win 7	45
		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
		(Googlebot(Oct 2013	65
		(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
		IE(7) - Vista	70
		IE(8) - XP	71
		IE(8) - XP	72
		IE(8) - Win 7	73
		IE(9) - Win 7	74
		IE(8-10) - Win 7	75
		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
		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
		(Java(6u45	97
		(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
		(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_RSA_WITH_AES_256_CBC_SHA256	tlsv1_2	Opera(12.15) - Win 7	105
		Opera(15) - Win 7	106
TLS_RSA_WITH_AES_256_CBC_SHA256	tlsv1_2	Opera(16) - Win 7	107
TLS_RSA_WITH_AES_256_CBC_SHA256	tlsv1_2	Opera(17) - Win 7	108
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	tlsv1_2	Safari(5) - iOS 5.1.1	109
		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
		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
		Tor(17.0.9) - Win 7	123
		(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
		(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

