

# بررسی SSL دامنه nedashimi.com

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

🕒 تاریخ تهیه گزارش : دوشنبه ۵ اسفند ۱۳۹۸ در ساعت ۱۶:۰۲  
👁 بازدید: 0

گزارش بررسی تنظیمات SSL دامنه nedashimi.com

☆ امتیاز: ★★★★★

HSTS



آسیب پذیری



سازگاری مرورگرها



معتبر



ارتباط تنها در SSL



اطلاعات هدر دامنه

Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8  
Vary: Accept-Encoding, Cookie  
Cache-Control: max-age=3, must-revalidate  
Last-Modified: Mon, 24 Feb 2020 12:06:48 GMT  
Content-Length: 27781  
Content-Encoding: gzip  
Date: Mon, 24 Feb 2020 12:32:46 GMT  
Alt-Svc: quic=":443"; ma=2592000; v="43,46", h3-Q043=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-24=":443"; ma=2592000, h3-25=":443"; ma=2592000



Shodan اطلاعات

## Shodan Information :

### 🔒 SSL Certificate

- Issued By:
  - |- Common Name:cPanel, Inc. Certification Authority
  - |- Organization:cPanel, Inc.
- Issued To:
  - |- Common Name:cp16-htz-230.ganjehost.com

### Supported SSL Versions

TLSv1.2

OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot \* ready.\* CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN A001 OK  
...Pre-login capabilities listed, post-login capabilities have mo

[cPanel Login](#)

138.201.137.230

cp16-htz-230.ganjehost.com

[Hetzner Online GmbH](#)

Added on 2020-02-13 06:45:45 GMT

[Germany](#) 🇩🇪

### SSL Certificate 🔒

:Issued By

Common Name:cPanel, Inc. Certification Authority -|

.Organization:cPanel, Inc -|

:Issued To

Common Name:cp16-htz-230.ganjehost.com -|

http://nedashimi.com/ -> 301 -> https://nedashimi.com/ -> 200  
 https://nedashimi.com/ -> 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

www.nedashimi.com	عنوان امضای دیجیتال :
IR - جمهوری اسلامی ایران	نام کشور :
www.nedashimi.com , nedashimi.com Alternative	عنوان های جایگزین امضا (Alternative) :
	Names :
جمعه ۱۰ خرداد ۱۳۹۸ در ساعت ۰۳:۱۰	شروع اعتبار از :
شنبه ۱۰ خرداد ۱۳۹۹ در ساعت ۰۳:۱۰ - اتمام در : 95 روز و 13 ساعت و 37 دقیقه و 27 ثانیه	پایان اعتبار تا :
Certum Domain Validation CA SHA2	صادر کننده مجوز :
PL - لهستان	کشور صادر کننده مجوز :
sha256 with RSA size: 2048 Bits	الگوریتم امضا :
(yes (certificate extension	Certificate Transparency :
OK - offered	OCSP stapling :
http://dvcasha2.ocsp-certum.com	OCSP URL :
http://crl.certum.pl/dvcasha2.crl	CRL Distribution Points :
	Trust
	Android iOS Java macOS Mozilla OPENJDK Windows
	بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

نام هاست دامنه : nedashimi.com

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 : =q55epZmMJBHS8qt3hERgdUF8dvgunVBSjauT8pnJJA

=Pin : q55epZmMJBHS8qt3hERgdUF8dvgunVBSjauT8pnJJA

Finger print : 46cc824d4ca8fbc9e20309dd04d00bd59c882c8b

عنوان : countryName=IR, commonName=www.nedashimi.com

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

سریال مجوز : 9.5884107249948E+37

شروع اعتبار از : 03:10:20 31-05-2019

پایان اعتبار تا : 03:10:20 30-05-2020

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

صادر کننده مجوز : 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

بلی : پشتیبانی از OCSF از \_\_\_

بلی : OCSF Response \_\_\_

بلی Trusted By Mozilla \_\_\_

: CA Store

C = PL, O = Asseco Data Systems S.A., CN = Certum Domain Validation CA SHA2 Validation Service : Responder ID \_\_\_

: Response Status \_\_\_

Feb 24 12:08:29 2020 GMT : Produced At \_\_\_

Type : DEFLATE - ندارد : Deflate Compression

(TLS Fallback Scsv) دارد : Downgrade Attacks Prevention

: Session Renegotiation

بلی : Secure Renegotiation \_\_\_

خیر Insecure Client-Initiated \_\_\_

: Renegotiation

: Resumption Support

ندارد Resumption With TLS \_\_\_

: Tickets

ندارد Resumption With Session \_\_\_

: IDs

Next Protocol Negotiation extension ارائه نشده است

: ((NPN

spdy/3.1http/1.1spdy/2spdy/3Application-Layer Protocol Negotiation

: ((ALPN

ارائه شده است (Personal Financial Specialist (PFS

: PFS Ciphers

ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305 ECDHE-RSA-AES128-GCM-SHA256

prime256v1 secp384r1 X25519

: PFS ECDHE curves

Default protocol TLS1.2

: Protocol Negotiated

(ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256

: Cipher Negotiated

renegotiation info/#65281 EC point formats/#11 session ticket/#35 status request/#5

: TLS Extensions

(valid for 7199 seconds only (< daily

: TLS Session Ticket

yes

: SSL SessionID Support

پشتیبانی می کند

: Session Resumption Ticket

پشتیبانی نمی کند

: Session Resumption ID

off by -14 seconds from your localtime

: TLS Timestamp

--

: DNS CAA Record

(yes (certificate extension

: Cert Transparency

( / ) OK 200

: HTTP Status

ارائه نشده است (HTTP Strict Transport Security (HSTS

:

!No Server banner line in header, interesting

: Banner Server

No support for HTTP Public Key Pinning

: (HTTP Public Key Pinning (HPKP

/ at 0

: Cookie Count

اطلاعات بیشتر

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 \_

no RSA key transport cipher , 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 \_

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

: BREACH

CVE-2013-3587

: CVE \_

CWE-310

: CVE \_

اطلاعات بیشتر

no protocol below TLS 1.2 offered

: Fallback SCSV

آسیب پذیر نیست

: POODLE SSL

CWE-310

: CVE \_

آسیب پذیر نیست

: SWEET32

CVE-2016-2183 CVE-2016-6329

: CVE \_

CWE-327

: CVE \_

[اطلاعات بیشتر ?](#)

آسیب پذیر نیست **FREAK (Factoring RSA Export : (Keys**

[اطلاعات بیشتر ?](#)

Make sure you don t use this certificate elsewhere with SSLv2 enabled services, see **DROWN (Decrypting RSA with Obsolete and : (Weakened eNcryption**  
<https://censys.io/ipv4?q=4241C8BDCF794651CED71EE36CB885EDDA4CD3E9C786F6ADCDE1FA6750E862B2>

CVE-2016-0800 CVE-2016-0703 : CVE \_|

CWE-310 : CWE \_|

no DH key with < = TLS 1.2 : **LOGJAM Common Primes**

CVE-2015-4000 : CVE \_|

CWE-310 : CWE \_|

[اطلاعات بیشتر ?](#)

,no DH EXPORT ciphers ,no DH EXPORT ciphers ,آسیب پذیر نیست : **LOGJAM**

CVE-2015-4000 : CVE \_|

CWE-310 : CWE \_|

[اطلاعات بیشتر ?](#)

no SSL3 or TLS1 ,آسیب پذیر نیست : **BEAST**

CVE-2011-3389 : CVE \_|

CWE-20 : CWE \_|

آسیب پذیر نیست : **LUCKY 13**

CVE-2013-0169 : CVE \_|

CWE-310 : CWE \_|

[اطلاعات بیشتر ?](#)

آسیب پذیر نیست : **RC4**

CWE-310 : 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			1
بلی	T	T	1
بلی	S	S	1

— 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 / Wrong version number	TLS_RSA_WITH_SEED_CBC_SHA	1
خیر	TLS / Wrong version number	TLS_RSA_WITH_RC4_128_SHA	2
خیر	TLS / Wrong version number	TLS_RSA_WITH_RC4_128_MD5	3
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	4
خیر	TLS / Wrong version number	TLS_RSA_WITH_NULL_SHA	5
خیر	TLS / Wrong version number	TLS_RSA_WITH_NULL_MD5	6
خیر	TLS / Wrong version number	TLS_RSA_WITH_IDEA_CBC_SHA	7
خیر	TLS / Wrong version number	TLS_RSA_WITH_DES_CBC_SHA	8
خیر	TLS / Wrong version number	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_RSA_WITH_AES_128_CBC_SHA	16
خیر	TLS / Wrong version number	TLS_RSA_WITH_3DES_EDE_CBC_SHA	17
خیر	TLS / Wrong version number	TLS_RSA_EXPORT_WITH_RC4_40_MD5	18

## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Wrong version number	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	100
خیر	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	107
خیر	TLS / Wrong version number	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	108
خیر	TLS / Wrong version number	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	109
خیر	TLS / Wrong version number	TLS_DHE_DSS_WITH_SEED_CBC_SHA	110
خیر	TLS / Wrong version number	TLS_DHE_DSS_WITH_DES_CBC_SHA	111
خیر	TLS / Wrong version number	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	112
خیر	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	119

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Wrong version number	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	120
خیر	TLS / Wrong version number	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	TLS / Alert: protocol version	TLS_RSA_WITH_SEED_CBC_SHA	1
خیر	TLS / Alert: protocol version	TLS_RSA_WITH_RC4_128_SHA	2
خیر	TLS / Alert: protocol version	TLS_RSA_WITH_RC4_128_MD5	3
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	4
خیر	TLS / Alert: protocol version	TLS_RSA_WITH_NULL_SHA	5
خیر	TLS / Alert: protocol version	TLS_RSA_WITH_NULL_MD5	6
خیر	TLS / Alert: protocol version	TLS_RSA_WITH_IDEA_CBC_SHA	7
خیر	TLS / Alert: protocol version	TLS_RSA_WITH_DES_CBC_SHA	8
خیر	TLS / Alert: protocol version	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	TLS / Alert: protocol version	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: protocol version	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: protocol version	TLS_RSA_WITH_AES_128_CBC_SHA	16
خیر	TLS / Alert: protocol version	TLS_RSA_WITH_3DES_EDE_CBC_SHA	17

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: protocol version	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	19
خیر	TLS / Alert: protocol version	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	20
بلی	TLS / Alert: protocol version	TLS_ECDH_anon_WITH_RC4_128_SHA	21
بلی	TLS / Alert: protocol version	TLS_ECDH_anon_WITH_NULL_SHA	22
بلی	TLS / Alert: protocol version	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	23
بلی	TLS / Alert: protocol version	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	24
بلی	TLS / Alert: protocol version	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	25
خیر	TLS / Alert: protocol version	TLS_ECDH_RSA_WITH_RC4_128_SHA	26
خیر	TLS / Alert: protocol version	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: protocol version	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: protocol version	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	33
خیر	TLS / Alert: protocol version	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	34
خیر	TLS / Alert: protocol version	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	35
خیر	TLS / Alert: protocol version	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	TLS / Alert: protocol version	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	TLS / Alert: protocol version	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	42
خیر	TLS / Alert: protocol version	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	43
خیر	TLS / Alert: protocol version	TLS_ECDHE_RSA_WITH_RC4_128_SHA	44
خیر	TLS / Alert: protocol version	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: protocol version	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: protocol version	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	51
خیر	TLS / Alert: protocol version	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	52
خیر	TLS / Alert: protocol version	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	53
خیر	TLS / Alert: protocol version	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: protocol version	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	TLS / Alert: protocol version	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	60
خیر	TLS / Alert: protocol version	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	61
بلی	TLS / Alert: protocol version	TLS_DH_anon_WITH_SEED_CBC_SHA	62
بلی	TLS / Alert: protocol version	TLS_DH_anon_WITH_RC4_128_MD5	63
بلی	TLS / Alert: protocol version	TLS_DH_anon_WITH_DES_CBC_SHA	64
بلی	TLS / Alert: protocol version	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	65
بلی	TLS / Alert: protocol version	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: protocol version	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: protocol version	TLS_DH_anon_WITH_AES_128_CBC_SHA	72
بلی	TLS / Alert: protocol version	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	73
بلی	TLS / Alert: protocol version	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	74
بلی	TLS / Alert: protocol version	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	75
خیر	TLS / Alert: protocol version	TLS_DH_RSA_WITH_SEED_CBC_SHA	76
خیر	TLS / Alert: protocol version	TLS_DH_RSA_WITH_DES_CBC_SHA	77
خیر	TLS / Alert: protocol version	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	78

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: protocol version	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	TLS / Alert: protocol version	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: protocol version	TLS_DH_RSA_WITH_AES_128_CBC_SHA	85
خیر	TLS / Alert: protocol version	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	86
خیر	TLS / Alert: protocol version	TLS_DH_DSS_WITH_SEED_CBC_SHA	87
خیر	TLS / Alert: protocol version	TLS_DH_DSS_WITH_DES_CBC_SHA	88
خیر	TLS / Alert: protocol version	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	89
خیر	TLS / Alert: protocol version	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: protocol version	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: protocol version	TLS_DH_DSS_WITH_AES_128_CBC_SHA	96
خیر	TLS / Alert: protocol version	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	97
خیر	TLS / Alert: protocol version	TLS_DHE_RSA_WITH_SEED_CBC_SHA	98

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: protocol version	TLS_DHE_RSA_WITH_DES_CBC_SHA	99
خیر	TLS / Alert: protocol version	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	100
خیر	TLS / Alert: protocol version	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: protocol version	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: protocol version	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	107
خیر	TLS / Alert: protocol version	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	108
خیر	TLS / Alert: protocol version	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	109
خیر	TLS / Alert: protocol version	TLS_DHE_DSS_WITH_SEED_CBC_SHA	110
خیر	TLS / Alert: protocol version	TLS_DHE_DSS_WITH_DES_CBC_SHA	111
خیر	TLS / Alert: protocol version	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	112
خیر	TLS / Alert: protocol version	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: protocol version	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	TLS / Alert: protocol version	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	119
خیر	TLS / Alert: protocol version	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	120
خیر	TLS / Alert: protocol version	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	TLS / Wrong version number	TLS_RSA_WITH_SEED_CBC_SHA	1
خیر	TLS / Wrong version number	TLS_RSA_WITH_RC4_128_SHA	2
خیر	TLS / Wrong version number	TLS_RSA_WITH_RC4_128_MD5	3
خیر	TLS / No ciphers available	TLS_RSA_WITH_NULL_SHA256	4
خیر	TLS / Wrong version number	TLS_RSA_WITH_NULL_SHA	5
خیر	TLS / Wrong version number	TLS_RSA_WITH_NULL_MD5	6
خیر	TLS / Wrong version number	TLS_RSA_WITH_IDEA_CBC_SHA	7
خیر	TLS / Wrong version number	TLS_RSA_WITH_DES_CBC_SHA	8
خیر	TLS / Wrong version number	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9
خیر	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_RSA_WITH_AES_128_CBC_SHA	16
خیر	TLS / Wrong version number	TLS_RSA_WITH_3DES_EDE_CBC_SHA	17



## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Wrong version number	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	19
خیر	TLS / Wrong version number	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	20
بلی	TLS / Wrong version number	TLS_ECDH_anon_WITH_RC4_128_SHA	21
بلی	TLS / Wrong version number	TLS_ECDH_anon_WITH_NULL_SHA	22
بلی	TLS / Wrong version number	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	23
بلی	TLS / Wrong version number	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	24
بلی	TLS / Wrong version number	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	25
خیر	TLS / Wrong version number	TLS_ECDH_RSA_WITH_RC4_128_SHA	26
خیر	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	33
خیر	TLS / Wrong version number	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	34
خیر	TLS / Wrong version number	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	35
خیر	TLS / Wrong version number	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	TLS / Wrong version number	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	TLS / Wrong version number	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	42
خیر	TLS / Wrong version number	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	43
خیر	TLS / Wrong version number	TLS_ECDHE_RSA_WITH_RC4_128_SHA	44
خیر	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	51
خیر	TLS / Wrong version number	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	52
خیر	TLS / Wrong version number	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	53
خیر	TLS / Wrong version number	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 / Wrong version number	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	TLS / Wrong version number	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	60
خیر	TLS / Wrong version number	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	61
بلی	TLS / Wrong version number	TLS_DH_anon_WITH_SEED_CBC_SHA	62
بلی	TLS / Wrong version number	TLS_DH_anon_WITH_RC4_128_MD5	63
بلی	TLS / Wrong version number	TLS_DH_anon_WITH_DES_CBC_SHA	64
بلی	TLS / Wrong version number	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	65
بلی	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_DH_anon_WITH_AES_128_CBC_SHA	72
بلی	TLS / Wrong version number	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	73
بلی	TLS / Wrong version number	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	74
بلی	TLS / Wrong version number	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	75
خیر	TLS / Wrong version number	TLS_DH_RSA_WITH_SEED_CBC_SHA	76
خیر	TLS / Wrong version number	TLS_DH_RSA_WITH_DES_CBC_SHA	77
خیر	TLS / Wrong version number	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	78

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Wrong version number	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	TLS / Wrong version number	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 / Wrong version number	TLS_DH_RSA_WITH_AES_128_CBC_SHA	85
خیر	TLS / Wrong version number	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	86
خیر	TLS / Wrong version number	TLS_DH_DSS_WITH_SEED_CBC_SHA	87
خیر	TLS / Wrong version number	TLS_DH_DSS_WITH_DES_CBC_SHA	88
خیر	TLS / Wrong version number	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	89
خیر	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_DH_DSS_WITH_AES_128_CBC_SHA	96
خیر	TLS / Wrong version number	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	97
خیر	TLS / Wrong version number	TLS_DHE_RSA_WITH_SEED_CBC_SHA	98

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Wrong version number	TLS_DHE_RSA_WITH_DES_CBC_SHA	99
خیر	TLS / Wrong version number	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	100
خیر	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	107
خیر	TLS / Wrong version number	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	108
خیر	TLS / Wrong version number	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	109
خیر	TLS / Wrong version number	TLS_DHE_DSS_WITH_SEED_CBC_SHA	110
خیر	TLS / Wrong version number	TLS_DHE_DSS_WITH_DES_CBC_SHA	111
خیر	TLS / Wrong version number	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	112
خیر	TLS / Wrong version number	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 / Wrong version number	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	TLS / Wrong version number	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	119
خیر	TLS / Wrong version number	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	120
خیر	TLS / Wrong version number	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	121

## : Accepted Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	1
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	2
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	3

## : Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	1

## : 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 / Alert: handshake failure	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_CAMELLIA_256_CBC_SHA256	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_SHA256	10
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	11
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_AES_256_GCM_SHA384	12
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_AES_256_CBC_SHA256	13
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_AES_256_CBC_SHA	14

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_AES_128_CBC_SHA256	16
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_AES_128_CBC_SHA	17
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_3DES_EDE_CBC_SHA	18
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_RC4_128_SHA	19
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_NULL_SHA	20
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	21
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	22
بلی	TLS / Alert: handshake failure	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	23
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_RC4_128_SHA	24
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_NULL_SHA	25
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	26
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	27
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	28
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	29
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	30
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	31
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	32
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	33
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_NULL_SHA	34
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	35



## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	36
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	37
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	38
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	39
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	40
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	41
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	42
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	43
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	44
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_SEED_CBC_SHA	45
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_RC4_128_MD5	46
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	47
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	48
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	49
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	50
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_GCM_SHA384	51
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA256	52
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA	53
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_GCM_SHA256	54
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA256	55

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA	56
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	57
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_SEED_CBC_SHA	58
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	59
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	60
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	61
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	62
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	63
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	64
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_256_CCM	65
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	66
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	67
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	68
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	69
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	70
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	71
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_SEED_CBC_SHA	72
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	73
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	74
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	75

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	76
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	77
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	78
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	79
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	80
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	81
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	82
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	83
خیر	TLS / Alert: handshake failure	RSA_WITH_AES_256_CCM_8	84
خیر	TLS / Alert: handshake failure	RSA_WITH_AES_256_CCM	85
خیر	TLS / Alert: handshake failure	RSA_WITH_AES_128_CCM_8	86
خیر	TLS / Alert: handshake failure	RSA_WITH_AES_128_CCM	87
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_256_CCM_8	88
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_256_CCM	89
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_128_CCM_8	90
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_128_CCM	91
خیر	TLS / Alert: handshake failure	ECDHE-ECDSA-ARIA256-GCM-SHA384	92
خیر	TLS / Alert: handshake failure	ECDHE-ECDSA-ARIA128-GCM-SHA256	93
خیر	TLS / Alert: handshake failure	ECDHE-ARIA256-GCM-SHA384	94
خیر	TLS / Alert: handshake failure	ECDHE-ARIA128-GCM-SHA256	95

## : Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	DHE_RSA_WITH_AES_256_CCM_8	96
خیر	TLS / Alert: handshake failure	DHE_RSA_WITH_AES_128_CCM_8	97
خیر	TLS / Alert: handshake failure	DHE_RSA_WITH_AES_128_CCM	98
خیر	TLS / Alert: handshake failure	DHE-RSA-ARIA256-GCM-SHA384	99
خیر	TLS / Alert: handshake failure	DHE-RSA-ARIA128-GCM-SHA256	100
خیر	TLS / Alert: handshake failure	DHE-DSS-ARIA256-GCM-SHA384	101
خیر	TLS / Alert: handshake failure	DHE-DSS-ARIA128-GCM-SHA256	102
خیر	TLS / Alert: handshake failure	ARIA256-GCM-SHA384	103
خیر	TLS / Alert: handshake failure	ARIA128-GCM-SHA256	104

: 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_CHACHA20_POLY1305_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
		Chrome(29) - Win 7	17
		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
		IE(11) - Win 7	77
		IE(11) - Win 7	78
		IE(11) - Win 7	79



: Handshake Simulation

Cipher	Type	Name	#
		IE(11) - Win 7	80
		IE(11) - Win 7	81
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 10 Preview	82
		IE(11) - Win 8.1	83
		IE(11) - Win 8.1	84
		IE(11) - Win 8.1	85
		IE(11) - Win 8.1	86
		IE(11) - Win 8.1	87
		IE(10) - Win Phone 8.0	88
		IE(11) - Win Phone 8.1	89
		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_GCM_SHA256	tlsv1_2	(Java(8b132	99

: Handshake Simulation

Cipher	Type	Name	#
TLS_ECDHE_RSA_WITH_AES_128_GCM_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
		Opera(12.15) - Win 7	105
		Opera(15) - Win 7	106
		Opera(16) - Win 7	107
		Opera(17) - Win 7	108
		Safari(5) - iOS 5.1.1	109
		Safari(5.1.9) - OS X 10.6.8	110
		Safari(6) - iOS 6.0.1	111
		Safari(6.0.4) - OS X 10.8.4	112
		Safari(7) - iOS 7.1	113
		Safari(8) - iOS 8.0 Beta	114
		Safari(7) - OS X 10.9	115
		Safari(8) - iOS 8.4	116
		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

