

بررسی SSL دامنه www.plustemplate.com

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

🕒 تاریخ تهیه گزارش : سه شنبه ۸ تیر ۱۴۰۰ در ساعت ۱۵:۲۹
👁 بازدید: 0

گزارش بررسی تنظیمات SSL دامنه www.plustemplate.com

🌟 امتیاز: ☆☆☆☆☆

HSTS



آسیب پذیری



سازگاری مرورگرها



معتبر



ارتباط تنها در SSL



اطلاعات هدر دامنه

```
Server: nginx
Date: Tue, 29 Jun 2021 10:59:00 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM", CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Content-Encoding: gzip
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-cache, no-store, no-cache, must-revalidate, max-age=0
Pragma: no-cache, no-cache, no-cache
Set-Cookie: d4dad69351632ac35975e3001dc7bbe8=15jkito5veq6fc0k8nj5elqj24; path=/; domain=plustemplate.com; HttpOnly
Content-Security-Policy: frame-src 'self' *.google-analytics.com
Last-Modified: Sat, 22 May 2021 12:37:20 GMT
ETag: "ceed1022bd8372bc4b9b2741fc9635ee"
X-Content-Type-Options: nosniff
X-Download-Options: noopen
Referrer-Policy: strict-origin-when-cross-origin
Strict-Transport-Security: max-age=16416000; includeSubdomains
Vary: User-Agent
```



اطلاعات Shodan

Shodan Information :

http://plustemplate.com/ -> 301 -> https://www.plustemplate.com/ -> 200

https://plustemplate.com/ -> 301 -> https://www.plustemplate.com/ -> 200

همیشه از HTTPS استفاده کنید

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

(HTTP Strict Transport Security (HSTS)

اطلاعات بیشتر

days (=16416000 seconds) > 15465600 seconds 190 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

plustemplate.com عنوان امضای دیجیتال :
, plustemplate.com , www.plustemplate.com Alternative) عنوان های جایگزین امضا
(Names :
یکشنبه ۰۲ خرداد ۱۴۰۰ در ساعت ۱۸:۵۲ شروع اعتبار از :
شنبه ۳۰ مرداد ۱۴۰۰ در ساعت ۱۸:۵۲ - اتمام در : 53 روز و 6 ساعت و 53 دقیقه و 9 ثانیه پایان اعتبار تا :
R3 صادر کننده مجوز :
US - ایالات متحده (آمریکا) کشور صادر کننده مجوز :
sha256 with RSA size: 4096 Bits الگوریتم امضا :
(yes (certificate extension : Certificate Transparency
LOW - not offered : OCSP stapling
http://r3.o.lencr.org : OCSP URL
-- : CRL Distribution Points
Trust
Android iOS Java macOS Mozilla OPENJDK Windows
بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

نام هاست دامنه : www.plustemplate.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 : =CM4IIR96II7iBgQTUW/JFxN6O8pSQkdBwAOG4qgJwlo

=Pin : CM4IIR96II7iBgQTUW/JFxN6O8pSQkdBwAOG4qgJwlo

Finger print : 0067cc9a83ba6df84305670eb4f170348573914a

عنوان : commonName=plustemplate.com

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

سریال مجوز : 2.8927962954905E+41

شروع اعتبار از : 18:52:13 23-05-2021

پایان اعتبار تا : 18:52:13 21-08-2021

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 : a053375bfe84e8b748782c7cee15827a6af5a405

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

صادر کننده مجوز : countryName=US, organizationName=Internet Security Research Group, commonName=ISRG Root X1

سریال مجوز : 1.9296149633997E+38

شروع اعتبار از : 00:00:00 04-09-2020

پایان اعتبار تا : 16:00:00 15-09-2025

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 3 : =C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M

=Pin : C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M

Finger print : cabd2a79a1076a31f21d253635cb039d4329a5e8

عنوان : countryName=US, organizationName=Internet Security Research Group, commonName=ISRG Root X1

صادر کننده مجوز : countryName=US, organizationName=Internet Security Research Group, commonName=ISRG Root X1

سریال مجوز : 1.7288692866979E+38

شروع اعتبار از : 11:04:38 04-06-2015

پایان اعتبار تا : 11:04:38 04-06-2035

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 4096

: OCSF Stapling

___ پشتیبانی از OCSF : خیر

___ OCSF Response : خیر

___ Trusted By Mozilla : خیر

: CA Store

Type : DEFLATE - ندارد : Deflate Compression

(TLS Fallback Scsv) دارد : Downgrade Attacks Prevention

: Session Renegotiation

___ Secure Renegotiation : بلی

___ Insecure Client-Initiated : خیر

: Renegotiation

: Resumption Support

دارد Resumption With TLS ___

: Tickets

دارد Resumption With Session ___

: IDs

___ تعداد کل تست های انجام شده : 5

___ تست های موفقیت آمیز : 5

___ تست های بدون پاسخ : 0

___ تعداد خطا ها : 0

Next Protocol Negotiation extension (with h2, http/1.1 (advertised شده است : (NPN

Application-Layer Protocol Negotiation : ((ALPN

Personal Financial Specialist (PFS) : ارائه شده است

ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256 : PFS Ciphers

prime256v1 : PFS ECDHE curves

ffdhe4096 : DH Groups

Default protocol TLS1.2 : Protocol Negotiated

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

server name/#0 renegotiation info/#65281 EC point formats/#11 session ticket/#35 heartbeat/#15 next protocol/#13172 : TLS Extensions

(valid for 300 seconds only (< daily : TLS Session Ticket

yes : SSL SessionID Support

پشتیبانی می کند : Session Resumption Ticket

پشتیبانی می کند : Session Resumption ID

off by -1 seconds from your localtime : TLS Timestamp

-- : DNS CAA Record

(yes (certificate extension : Cert Transparency

(/) OK 200 : HTTP Status

days (=16416000 seconds) > 15465600 seconds 190 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

nginx : Banner Server

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

/ at 1 : Cookie Count

at / marked as secure 0/1 : Cookie Secure

All (1) at / marked as HttpOnly : Cookie HTTP Only

آسیب پذیر نیست , timed out : Heartbleed

آسیب پذیر نیست : (Certified Coding Specialist (CCS

returned potential memory fragments do not differ , 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-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 _|

اطلاعات بیشتر

	آسیب پذیر نیست	Compression Ratio Info-leak
	CVE-2012-4929	: CVE _
	CWE-310	: CVE _
	ممکن است آسیب پذیر باشد, <i>uses gzip HTTP compression - only supplied / tested</i>	: BREACH
	CVE-2013-3587	: CVE _
	CWE-310	: CVE _
	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 _
	آسیب پذیر نیست	FREAK (Factoring RSA Export
		: (Keys
	Make sure you don t use this certificate elsewhere with SSLv2 enabled services, see DROWN (Decrypting RSA	DROWN (Decrypting RSA
	https://censys.io/ipv4?with=Obsolete and Weakened	with Obsolete and Weakened
	q=B75C8D10E5221F0FF9278C7342BE6CC02631AC63E432E0665F16B3BEA93FE299	: (e)ncryption
	CVE-2016-0800 CVE-2016-0703	: CVE _
	CWE-310	: CVE _
	RFC7919/ffdhe4096	: LOGJAM Common Primes
	CVE-2015-4000	: CVE _
	CWE-310	: CVE _
	آسیب پذیر نیست, <i>no DH EXPORT ciphers</i>	: LOGJAM
	CVE-2015-4000	: CVE _
	CWE-310	: CVE _
	آسیب پذیر نیست, <i>no SSL3 or TLS1</i>	: BEAST
	CVE-2011-3389	: CVE _
	CWE-20	: CVE _
	آسیب پذیر نیست	: LUCKY 13
	CVE-2013-0169	: CVE _
	CWE-310	: CVE _
	آسیب پذیر نیست	: RC4
	CWE-310	: CVE _

اطلاعات بیشتر

اطلاعات بیشتر

اطلاعات بیشتر

اطلاعات بیشتر

اطلاعات بیشتر

اطلاعات بیشتر

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

: Accepted Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	1
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	2
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	3
خیر	HTTP 200 OK	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	4

: 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

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_RSA_WITH_AES_128_GCM_SHA256	15
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_CHACHA20_POLY1305_SHA256	26
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	27
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	28
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	29
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	30
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	31
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	32
خیر	TLS / Alert: handshake failure	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	33
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	34

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_NULL_SHA	35
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	36
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	37
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	38
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	39
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	40
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	41
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	42
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	43
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	44
خیر	TLS / Alert: handshake failure	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	45
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_SEED_CBC_SHA	46
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_RC4_128_MD5	47
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	48
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	49
بلی	TLS / No ciphers available	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	50
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	51
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_GCM_SHA384	52
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA256	53
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_256_CBC_SHA	54

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_GCM_SHA256	55
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA256	56
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_AES_128_CBC_SHA	57
بلی	TLS / Alert: handshake failure	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	58
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_SEED_CBC_SHA	59
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	60
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	61
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	62
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	63
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	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_CBC_SHA256	68
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	69
خیر	TLS / Alert: handshake failure	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	70
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_SEED_CBC_SHA	71
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	72
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	73
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	74

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	75
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	76
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	77
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	78
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	79
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	80
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	81
خیر	TLS / Alert: handshake failure	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	82
خیر	TLS / Alert: handshake failure	RSA_WITH_AES_256_CCM_8	83
خیر	TLS / Alert: handshake failure	RSA_WITH_AES_256_CCM	84
خیر	TLS / Alert: handshake failure	RSA_WITH_AES_128_CCM_8	85
خیر	TLS / Alert: handshake failure	RSA_WITH_AES_128_CCM	86
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_256_CCM_8	87
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_256_CCM	88
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_128_CCM_8	89
خیر	TLS / Alert: handshake failure	ECDHE_ECDSA_WITH_AES_128_CCM	90
خیر	TLS / Alert: handshake failure	ECDHE-ECDSA-ARIA256-GCM-SHA384	91
خیر	TLS / Alert: handshake failure	ECDHE-ECDSA-ARIA128-GCM-SHA256	92
خیر	TLS / Alert: handshake failure	ECDHE-ARIA256-GCM-SHA384	93
خیر	TLS / Alert: handshake failure	ECDHE-ARIA128-GCM-SHA256	94

: Rejected Cipher Suites

Anonymous	Connection Status	Name	#
خیر	TLS / Alert: handshake failure	DHE_RSA_WITH_AES_256_CCM_8	95
خیر	TLS / Alert: handshake failure	DHE_RSA_WITH_AES_128_CCM_8	96
خیر	TLS / Alert: handshake failure	DHE_RSA_WITH_AES_128_CCM	97
خیر	TLS / Alert: handshake failure	DHE-RSA-ARIA256-GCM-SHA384	98
خیر	TLS / Alert: handshake failure	DHE-RSA-ARIA128-GCM-SHA256	99
خیر	TLS / Alert: handshake failure	DHE-DSS-ARIA256-GCM-SHA384	100
خیر	TLS / Alert: handshake failure	DHE-DSS-ARIA128-GCM-SHA256	101
خیر	TLS / Alert: handshake failure	ARIA256-GCM-SHA384	102
خیر	TLS / Alert: handshake failure	ARIA128-GCM-SHA256	103

: 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
		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
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 7	78
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 7	79

: Handshake Simulation

Cipher	Type	Name	#
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 7	80
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	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
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 8.1	84
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 8.1	85
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 8.1	86
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	tlsv1_2	IE(11) - Win 8.1	87
		IE(10) - Win Phone 8.0	88
		IE(11) - Win Phone 8.1	89
TLS_DHE_RSA_WITH_AES_256_GCM_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_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

