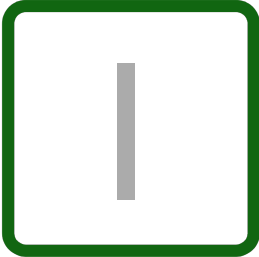


Scan Summary



Host:	www.apple.com (104.97.44.213)
Scan ID #:	55571128
End Time:	June 24, 2023 2:24 AM
Compatibility Level:	Intermediate
Certificate Explainer:	189029349

Certificate Information

Common name:	www.apple.com
Alternative Names:	www.apple.com, images.apple.com, www.apple.com.cn
First Observed:	2023-05-03 (certificate # 189029349)
Valid From:	2023-05-02
Valid To:	2023-10-28
Key:	RSA 2048 bits
Issuer:	Apple Public EV Server RSA CA 2 - G1
Signature Algorithm:	SHA256WithRSA

Cipher Suites

Cipher Suite	Code()	Key size	AEAD()	PFS()	Protocols
ECDHE-RSA-AES256-GCM-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x2F	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-SHA384	0x0C 0x28	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES128-SHA256	0x0C 0x27	2048 bits	✗	✓	TLS 1.2
ECDHE-RSA-AES256-SHA	0x0C 0x14	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
ECDHE-RSA-AES128-SHA	0x0C 0x13	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES256-GCM-SHA384	0x00 0x9D	2048 bits	✓	✗	TLS 1.2
RSA-AES128-GCM-SHA256	0x00 0x9C	2048 bits	✓	✗	TLS 1.2
RSA-AES256-SHA256	0x00 0x3D	2048 bits	✗	✗	TLS 1.2

Cipher Suite	Code	Key size	AEAD	PFS	Protocols
RSA-AES128-SHA256	0x00 0x3C	2048 bits	✗	✗	TLS 1.2
RSA-AES256-SHA	0x00 0x35	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES128-SHA	0x00 0x2F	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0

Miscellaneous Information	
CAA Record:	Yes, on apple.com
Cipher Preference:	Server selects preferred cipher
Compatible Clients:	Android 2.3.7, Apple ATS 9, Baidu Jan 2015, BingBot Dec 2013, BingPreview Dec 2013, Chrome 27, Edge 12, Firefox 21, Googlebot Oct 2013, IE 7, Java 6u45, OpenSSL 0.9.8y, Opera 12.15, Safari 5, Tor 17.0.9, Yahoo Slurp Oct 2013, YandexBot May 2014
OCSP Stapling:	Yes

Suggestions	
Looking for improved security and have a user base of only modern clients?	
Take a look at the Mozilla “Modern” TLS configuration ! It provides an extremely high level of security and performance and is compatible with all clients released in the last couple years. It is not recommended for general purpose websites that may need to service older clients such as Android 4.x, Internet Explorer 10, or Java 6.x.	
Want the detailed technical nitty-gritty?	
Please note that these suggestions may not be appropriate for your particular usage requirements! If they do sound like something you'd like assistance with, then hop on board:	
Teleport me to Mozilla's configuration generator!	