

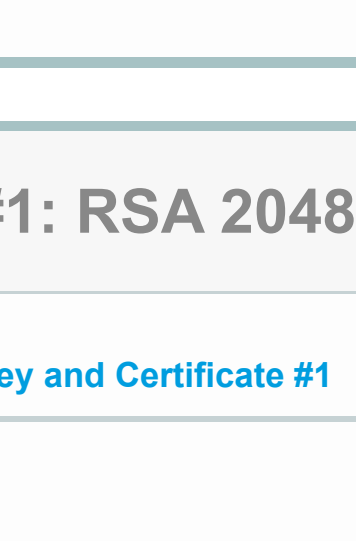
You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > mastermind-be.azurewebsites.net

SSL Report: mastermind-be.azurewebsites.net (20.50.2.23)



Assessed on: Tue, 01 Jun 2021 15:08:01 UTC | [HIDDEN](#) | [Clear cache](#)






Summary

Overall Rating







Certificate #1: RSA 2048 bits (SHA256withRSA)

	Server Key and Certificate #1	
Subject	*.azurewebsites.net Fingerprint SHA256: 73e3c312a3a0ac076364b27ebca79da274f5179a43573e3a12b2ba201f6931e Pin SHA256: VEGzzyvWjDWhY4p0Kx0425M[Yv5JnuPXKQJJC2SQ=	
Common names	*.azurewebsites.net	
Alternative names	*.azurewebsites.net *.scm.azurewebsites.net *.azure-mobile.net *.scm.azure-mobile.net *.sso.azurewebsites.net	
Serial Number	6b0000312fb373bc1b93bc837900000000312f	
Valid from	Mon, 28 Sep 2020 19:00:01 UTC	
Valid until	Tue, 28 Sep 2021 19:00:01 UTC (expires in 3 months and 27 days)	
Key	RSA 2048 bits (e 65537)	
Weak key (Debian)	No	
Issuer	Microsoft RSA TLS CA 01 AIA: http://www.microsoft.com/pki/mscorp/Microsoft%20RSA%20TLS%20CA%2001.crl	
Signature algorithm	SHA256withRSA	
Extended Validation	No	
Certificate Transparency	Yes (certificate)	
OCSP Must Staple	No	
Revocation information	CRL: OCSP CRL: http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl CRL: http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl OCSP: http://ocsp.msocsp.com	
Revocation status	Good (not revoked)	
DNS CAA	No (more info)	
Trusted	Yes Mozilla Apple Android Java Windows	

	Additional Certificates (if supplied)	
Certificates provided	2 (3411 bytes)	
Chain issues	None	
#2		
Subject	Microsoft RSA TLS CA 01 Fingerprint SHA256: 04eeea8e50a4775b3c24797282917ee5002eac4c75b56cdf3ee1c18fca5ba52 Pin SHA256: aJfLgIq2RMTfDuK1Y2Y68uYH6daff7O6i4ckcs=	
Valid until	Tue, 08 Oct 2024 07:00:00 UTC (expires in 3 years and 4 months)	
Key	RSA 4096 bits (e 65537)	
Issuer	Baltimore CyberTrust Root	
Signature algorithm	SHA256withRSA	
		
	Certification Paths	
Mozilla	Apple	Android
Java	Windows	
Path #1: Trusted		
1	Sent by server	*.azurewebsites.net Fingerprint SHA256: 73e3c312a3a0ac076364b27ebca79da274f5179a43573e3a12b2ba201f6931e Pin SHA256: VEGzzyvWjDWhY4p0Kx0425M[Yv5JnuPXKQJJC2SQ=
2	Sent by server	Microsoft RSA TLS CA 01 Fingerprint SHA256: 04eeea8e50a4775b3c24797282917ee5002eac4c75b56cdf3ee1c18fca5ba52 Pin SHA256: aJfLgIq2RMTfDuK1Y2Y68uYH6daff7O6i4ckcs=
3	In trust store	Baltimore CyberTrust Root Self-signed Fingerprint SHA256: 16af57a9b76b0ab128055a5ebade722ab31119d544ac95c493db0f026aeb Pin SHA256: Y8mvm0ex8k1Jc0D57f6/vm28k0dFmfw0KcVnYx0u80p=
		RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

	Protocols	
TLS 1.3	No	
TLS 1.2	Yes	
TLS 1.1	No	
TLS 1.0	No	
SSL 3	No	
SSL 2	No	
	Cipher Suites	
# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK 128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x3f)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128

	Handshake Simulation	
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 8u101	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.1 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.2a R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1 FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS 10 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)


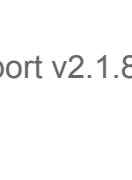

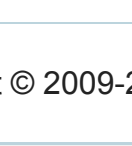
Android 2.3.7	No SNI ²	Protocol mismatch (not simulated)
Android 4.0.4		Protocol mismatch (not simulated)
Android 4.1.1		Protocol mismatch (not simulated)
Android 4.2.2		Protocol mismatch (not simulated)
Android 4.3		Protocol mismatch (not simulated)
Baidu Jan 2015		Protocol mismatch (not simulated)
IE 6 / XP	No FS ¹ No SNI ²	Protocol mismatch (not simulated)
IE 7 / Vista		Protocol mismatch (not simulated)
IE 8 / XP	No FS ¹ No SNI ²	Protocol mismatch (not simulated)
IE 8-10 / Win 7 R		Protocol mismatch (not simulated)
IE 10 / Win Phone 8.0		Protocol mismatch (not simulated)
Java 6u45	No SNI ²	Protocol mismatch (not simulated)
Java 7u25		Protocol mismatch (not simulated)
OpenSSL 0.9.8y		Protocol mismatch (not simulated)
Safari 5.1.9 / OS X 10.6.8		Protocol mismatch (not simulated)
Safari 6.0.4 / OS X 10.8.4 R		Protocol mismatch (not simulated)

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

	Protocol Details	
DROWN	No, server keys and hostname not seen elsewhere with this (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete	
Secure Renegotiation	Supported	
Secure Client-Initiated Renegotiation	No	
Insecure Client-Initiated Renegotiation	No	
BEAST attack	Mitigated server-side (more info)	
POODLE (SSLv3)	No, SSL 3 not supported (more info)	
POODLE (TLS)	No (more info)	
Zombie POODLE	No (more info) TLS 1.2 : 0xc027	
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027	
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027	
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027	
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)	
SSL/TLS compression	No	
RC4	No	
Heartbeat (extension)	No	
Heartbleed (vulnerability)	No (more info)	
Ticketbleed (vulnerability)	No (more info)	
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)	
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)	
ROBOT (vulnerability)	No (more info)	
Forward Secrecy	Yes (with most browsers) ROBUST (more info)	
ALPN	No	
NPN	No	
Session resumption (caching)	No (IDs assigned but not accepted)	
Session resumption (tickets)	No	
OCSP stapling	Yes	
Strict Transport Security (HSTS)	No	
HSTS Preloading	Not in: Chrome Edge Firefox IE	
Public Key Pinning (HPKP)	No (more info)	
Public Key Pinning Report-Only	No	
Public Key Pinning (Static)	No (more info)	
Long handshake intolerance	No	
TLS extension intolerance	No	
TLS version intolerance	No	
Incorrect SNI alerts	No	
Uses common DH primes	No, DHE suites not supported	
DH public server param (Ys) reuse	No, DHE suites not supported	
ECDDH public server param reuse	No	
Supported Named Groups	secp256r1, secp384r1 (server preferred order)	
SSL 2 handshake compatibility	No	
	HTTP Requests	
1	https://mastermind-be.azurewebsites.net/ (HTTP/1.1 200 OK)	
Content-Length	20	
Content-Type	application/json; charset=utf-8	
Date	Tue, 01 Jun 2021 15:06:18 GMT	
Connection	close	
	Miscellaneous	
Test date	Tue, 01 Jun 2021 15:06:06 UTC	
Test duration	114.691 seconds	
HTTP status code	200	
HTTP server signature	-	
Server hostname	-	