SSL Report: nosql.ru (188.244.7.47)

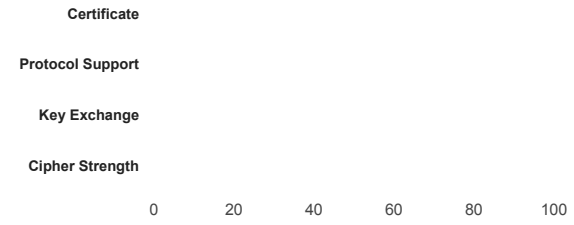
Assessed on: Thu, 20 Mar 2025 12:55:56 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Certificate #1: EC 384 bits (SHA384withECDSA)

Server Key and Certificate #1

Subject	nosql.ru Fingerprint SHA256: beeac226f62bde80c157b15e49445f3c4a4f297e3b10dadae421d7382e2ff6aa Pin SHA256: CDNDTGJpN+DMkyDLcW/oeVBoxU6i2WmaJu0JxHUNDj8=
Common names	nosql.ru
Alternative names	*.nosql.ru nosql.ru
Serial Number	06a955e7d08a1bf602b299745387f45e86ad
Valid from	Mon, 17 Mar 2025 20:52:10 UTC
Valid until	Sun, 15 Jun 2025 20:52:09 UTC (expires in 2 months and 26 days)
Key	EC 384 bits
Weak key (Debian)	No
Issuer	E6 AIA: http://e6.i.lencr.org/
Signature algorithm	SHA384withECDSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://e6.c.lencr.org/46.crl OCSP: http://e6.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2091 bytes)
Chain issues	None

Additional Certificates (if supplied)

#2

Subject	E6 Fingerprint SHA256: 76e9e288aafc0e37f4390cbf946aad997d5c1c901b3ce513d3d8fadbabe2ab85 Pin SHA256: 0Bbh/jEZSKymTy3kTOhsmlHKBB32EDu1KojrP3YfV9c=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 1 year and 11 months)
Key	EC 384 bits
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	nosql.ru Fingerprint SHA256: beeac226f62bde80c157b15e49445f3c4a4f297e3b10dadae421d7382e2ff6aa Pin SHA256: CDNDTGJpN+DMkyDLcW/oeVBoxU6i2WmaJu0JxHUNDj8= EC 384 bits / SHA384withECDSA
2	Sent by server	E6 Fingerprint SHA256: 76e9e288aafc0e37f4390cbf946aad997d5c1c901b3ce513d3d8fadbabe2ab85 Pin SHA256: 0Bbh/jEZSKymTy3kTOhsmlHKBB32EDu1KojrP3YfV9c= EC 384 bits / SHA256withRSA
3	In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

Certificate #2: EC 384 bits (SHA384withECDSA) No SNI

Server Key and Certificate #1

Subject	itwrks.org Fingerprint SHA256: 664cdcc6322639f6c084172d11581556ef58a5468c36f0afded3bd86a7dac758 Pin SHA256: ro4WQH0WFFNqStd2wm6HWjfHZw65+oiq0N9lueY6Xik=
Common names	itwrks.org
Alternative names	*.itwrks.org itwrks.org **MISMATCH**
Serial Number	0412253d9def0dba5da8945c49927c238fcb
Valid from	Mon, 10 Mar 2025 20:14:15 UTC
Valid until	Sun, 08 Jun 2025 20:14:14 UTC (expires in 2 months and 19 days)
Key	EC 384 bits
Weak key (Debian)	No
Issuer	E5 AIA: http://e5.i.lencr.org/
Signature algorithm	SHA384withECDSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://e5.o.lencr.org
Revocation status	Good (not revoked)
Trusted	No **NOT TRUSTED** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	2 (2046 bytes)
Chain issues	None

#2

Subject	E5 Fingerprint SHA256: 5dfdb3cf31b26f23d87c09f3a0cef642f64069a9fb7cfe29270bb5dc0f1e16bb

Additional Certificates (if supplied)

	Pin SHA256: NYbU7PBwV4y9J67c4guWTki8FJ+uudrXL0a4V4aRcrg=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 1 year and 11 months)
Key	EC 384 bits
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla Apple Android Java Windows

Path #1: Not trusted (invalid certificate [Fingerprint SHA256: 664cdcc6322639f6c084172d11581556ef58a5468c36f0afded3bd86a7dac758])

1	Sent by server	itwrks.org Fingerprint SHA256: 664cdcc6322639f6c084172d11581556ef58a5468c36f0afded3bd86a7dac758 Pin SHA256: ro4WQH0WFFNqStd2wm6HWjfHZw65+oiq0N9lueY6Xik= EC 384 bits / SHA384withECDSA
2	Sent by server	E5 Fingerprint SHA256: 5dfdb3cf31b26f23d87c09f3a0cef642f64069a9fb7cfe29270bb5dc0f1e16bb Pin SHA256: NYbU7PBwV4y9J67c4guWTki8FJ+uudrXL0a4V4aRcrg= EC 384 bits / SHA256withRSA
3	In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

 # TLS 1.3 (server has no preference)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH secp384r1 (eq. 7680 bits RSA) FS	256

 # TLS 1.2 (server has no preference)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH secp384r1 (eq. 7680 bits RSA) FS	256

Handshake Simulation

Android 4.4.2	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Android 5.0.0	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Android 6.0	EC 384 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Android 7.0	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Android 8.0	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS

Handshake Simulation

BingPreview Jan 2015	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Chrome 49 / XP SP3	Server sent fatal alert: handshake_failure		
Chrome 69 / Win 7 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp384r1 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp384r1 FS
Firefox 31.3.0 ESR / Win 7	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Firefox 47 / Win 7 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Firefox 49 / XP SP3	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Firefox 62 / Win 7 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp384r1 FS
Googlebot Feb 2018	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
IE 11 / Win 7 R	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
IE 11 / Win 8.1 R	EC 384 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
IE 11 / Win Phone 8.1 R	EC 384 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp384r1 FS
IE 11 / Win Phone 8.1 Update R	EC 384 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
IE 11 / Win 10 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 15 / Win 10 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 16 / Win 10 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 18 / Win 10 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Edge 13 / Win Phone 10 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Java 8u161	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp384r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp384r1 FS
OpenSSL 1.0.1l R	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
OpenSSL 1.0.2s R	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
OpenSSL 1.1.0k R	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure		
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure		
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure		
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure		
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure		
Safari 9 / iOS 9 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 9 / OS X 10.11 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 10 / iOS 10 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 10 / OS X 10.12 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH secp384r1 FS
Apple ATS 9 / iOS 9 R	EC 384 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
Yahoo Slurp Jan 2015	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
YandexBot Jan 2015	EC 384 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 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)

Handshake Simulation

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

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)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
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	Yes h2 http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	**Yes** max-age=31536000; includeSubDomains
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
ECDH public server param reuse	No
Supported Named Groups	secp384r1
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 **https://nosql.ru/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Thu, 20 Mar 2025 12:54:16 UTC
Test duration	100.24 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	www.itwrks.org

SSL Report v2.3.1