You are here: Home > Projects > SSL Server Test > www.dbj.jp > 202.230.205.12

SSL Report: www.dbj.jp (202.230.205.12)

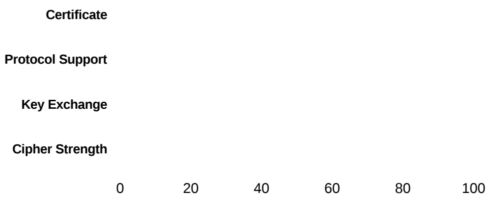
Assessed on: Tue, 26 Feb 2019 17:09:02 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



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

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.dbj.jp Fingerprint SHA256: d990e6c4b1a173c6ef24da2c657eddd7660707db8e4d8207dab69e12cb1c40de Pin SHA256: QSexS40HmSphQRr6N12Chgotn30Is05mGN+/9LJmIiY=
Common names	*.dbj.jp
Alternative names	*.dbj.jp dbj.jp
Serial Number	195bf54fafd43db6d3ea4b31
Valid from	Sat, 31 Mar 2018 15:00:00 UTC
Valid until	Sun, 31 Mar 2019 14:59:59 UTC (expires in 1 month and 4 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GlobalSign Organization Validation CA - SHA256 - G2 AIA: http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl OCSP: http://ocsp2.globalsign.com/gsorganizationvalsha2g2
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	2 (2917 bytes)

Additional Certificates (if supplied)

Chain issues	None

#2

Subject	GlobalSign Organization Validation CA - SHA256 - G2 Fingerprint SHA256: 74ef335e5e18788307fb9d89cb704bec112abd23487dbff41c4ded5070f241d9 Pin SHA256: IQBnNBEiFuhj+8x6X8XLgh01V9Ic5/V3IRQLNFFc7v4=
Valid until	Tue, 20 Feb 2024 10:00:00 UTC (expires in 4 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA

Certification Paths ⊞

Click here to expand

Configuration

Protocols

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

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suites

# TLS 1.2 (suites in server-preferred order) ⊟

TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128

# TLS 1.1 (suites in server-preferred order) ⊞

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No 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_RSA_WITH_AES_256_GCM_SHA384 No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No 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_RSA_WITH_AES_256_GCM_SHA384 No FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS

Handshake Simulation

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_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256	No FS

# Not simulated clients (Protocol mismatch)

Click here to expand

(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 SSLv2 **(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
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
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)

Protocol Details

ROBOT (vulnerability)	No (more info)
Forward Secrecy	**With some browsers** (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
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
ECDH public server param reuse	No
Supported Named Groups	secp256r1
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://www.dbj.jp/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Tue, 26 Feb 2019 17:06:50 UTC
Test duration	131.828 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	-

SSL Report v1.32.16

Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.