QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > secure1.bpiexpressonline.com

SSL Report: secure1.bpiexpressonline.com (203.161.188.164)

Assessed on: Fri, 27 Nov 2015 18:42:59 UTC | Clear cache

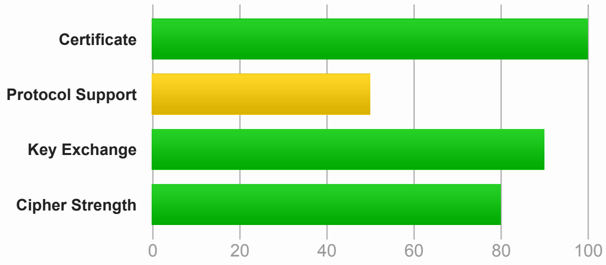
Scan Another »

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »



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

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	secure1.bpiexpressonline.com Fingerprint SHA1: b04ab68220107c9d74c0106cacdd660dfafc623d Pin SHA256: JxHWwL/tMPW8FeHUCNhAj5kwF/Mq4ZC03zHY0/WEg0c=
Common names	secure1.bpiexpressonline.com
Alternative names	secure1.bpiexpressonline.com
Prefix handling	Not required for subdomains
Valid from	Tue, 11 Aug 2015 00:00:00 UTC
Valid until	Wed, 10 Aug 2016 23:59:59 UTC (expires in 8 months and 14 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Symantec Class 3 EV SSL CA - G3
Signature algorithm	SHA256withRSA
Extended Validation	**Yes**
Certificate Transparency	**Yes (certificate)**
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	**Yes**

Additional Certificates (if supplied)

Certificates provided	2 (2981 bytes)
Chain issues	None

#2

Subject	Symantec Class 3 EV SSL CA - G3 Fingerprint SHA1: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12 Pin SHA256: gMxWOrX4PMQesK9qFNbYBxjBfjUvlkn/vN1n+L9lE5E=
Valid until	Mon, 30 Oct 2023 23:59:59 UTC (expires in 7 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA256withRSA

Certification Paths

Path #1: Trusted

1	Sent by server	secure1.bpiexpressonline.com Fingerprint SHA1: b04ab68220107c9d74c0106cacdd660dfafc623d Pin SHA256: JxHWwL/tMPW8FeHUCNhAj5kwF/Mq4ZC03zHY0/WEg0c= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	Symantec Class 3 EV SSL CA - G3 Fingerprint SHA1: e3fc0ad84f2f5a83ed6f86f567f8b14b40dcbf12 Pin SHA256: gMxWOrX4PMQesK9qFNbYBxjBfjUvlkn/vN1n+L9lE5E= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	VeriSign Class 3 Public Primary Certification Authority - G5 Self-signed Fingerprint SHA1: 4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 Pin SHA256: JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

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

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_RSA_WITH_RC4_128_MD5 (0x4) **INSECURE**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **INSECURE**	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.1.1	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.2.2	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.3	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 4.4.2	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Android 5.0.0	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Baidu Jan 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
BingPreview Jan 2015	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Chrome 45 / OS X R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Firefox 31.3.0 ESR / Win 7	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Firefox 41 / OS X R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112

Googlebot Feb 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 6 / XP No FS [1] No SNI [2]	Protocol or cipher suite mismatch		Fail[3]
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 8 / XP No FS [1] No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 11 / Win 7 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 11 / Win 8.1 R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
IE 10 / Win Phone 8.0	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
IE 11 / Win Phone 8.1 R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
IE 11 / Win Phone 8.1 Update R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
IE 11 / Win 10 R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Edge / Win 10 R	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112
Java 6u45 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Java 8u31	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
OpenSSL 1.0.1l R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
OpenSSL 1.0.2 R	Protocol or cipher suite mismatch		Fail[3]
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 6 / iOS 6.0.1 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 7 / iOS 7.1 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 7 / OS X 10.9 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 8 / iOS 8.4 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 8 / OS X 10.10 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 9 / iOS 9 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Safari 9 / OS X 10.11 R	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128
Apple ATS 9 / iOS 9 R	Protocol or cipher suite mismatch		Fail[3]
Yahoo Slurp Jan 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5) No FS RC4	128
YandexBot Jan 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_MD5 (0x4) No FS RC4	128

(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 tend to 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).

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info) TLS 1.0: 0x4
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Unknown (requires support for at least two protocols)
SSL/TLS compression	No
RC4	**Yes INSECURE** (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
Forward Secrecy	**No WEAK** (more info)
Next Protocol Negotiation (NPN)	No
Session resumption (caching)	Yes

Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor secure1.bpiexpressonline.com
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
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
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Fri, 27 Nov 2015 18:41:52 UTC
Test duration	67.824 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/6.0
Server hostname	-

SSL Report v1.20.28

Terms and Conditions