You are here: Home > Projects > SSL Server Test > eastwestpersonal.com.ph > 203.177.229.123

SSL Report: eastwestpersonal.com.ph (203.177.229.123)

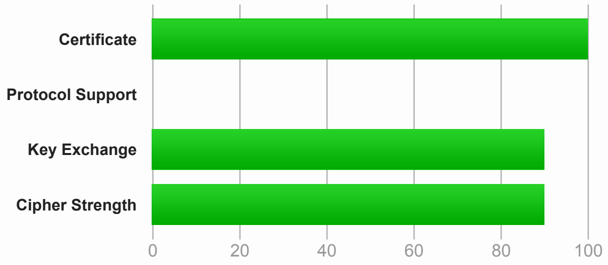
Assessed on: Fri, 27 Nov 2015 18:47:51 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server is vulnerable to the POODLE TLS attack. Patching required. Grade set to F. MORE INFO »

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

This server uses RC4 with modern protocols. Grade capped to C.

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

Authentication

Server Key and Certificate #1

Subject	www.eastwestpersonal.com.ph Fingerprint SHA1: 956455fed625e00e7413e6dcbf776633e785fd1a Pin SHA256: KXc3OErgO6WtQ9MnWeApehII9h5Ojaz3mWbieudciWs=
Common names	www.eastwestpersonal.com.ph
Alternative names	www.eastwestpersonal.com.ph
Prefix handling	Not valid for "eastwestpersonal.com.ph" **CONFUSING**
Valid from	Wed, 18 Dec 2013 00:00:00 UTC
Valid until	Mon, 21 Dec 2015 23:59:59 UTC (expires in 24 days, 5 hours)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	VeriSign Class 3 Extended Validation SSL SGC CA
Signature algorithm	SHA1withRSA **WEAK**
Extended Validation	**Yes** **No CT information provided** (more info)
Certificate Transparency	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	**Yes**

Additional Certificates (if supplied)

Certificates provided	3 (4312 bytes)
Chain issues	Extra certs

#2

Subject	VeriSign Class 3 Extended Validation SSL SGC CA Fingerprint SHA1: b18039899831f152614667cf23ffcea2b0e73dab Pin SHA256: TfUknRoG8EPFF/IfejfY9nW2CPiv9v5p3/1WM2e0urg=
Valid until	Mon, 07 Nov 2016 23:59:59 UTC (expires in 11 months and 11 days)
Key	RSA 2048 bits (e 65537)
Issuer	VeriSign Class 3 Public Primary Certification Authority - G5
Signature algorithm	SHA1withRSA **WEAK**

#3

Subject	VeriSign Class 3 Public Primary Certification Authority - G5 Fingerprint SHA1: 32f30882622b87cf8856c63db873df0853b4dd27 Pin SHA256: JbQbUG5JMJUoI6brnx0x3vZF6jilxsapbXGVfjhN8Fg=
Valid until	Sun, 07 Nov 2021 23:59:59 UTC (expires in 5 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	VeriSign, Inc. / Class 3 Public Primary Certification Authority
Signature algorithm	SHA1withRSA **WEAK**

Certification Paths

Path #1: Trusted

1	Sent by server	www.eastwestpersonal.com.ph Fingerprint SHA1: 956455fed625e00e7413e6dcbf776633e785fd1a Pin SHA256: KXc3OErgO6WtQ9MnWeApehII9h5Ojaz3mWbieudciWs= RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
2	Sent by server	VeriSign Class 3 Extended Validation SSL SGC CA Fingerprint SHA1: b18039899831f152614667cf23ffcea2b0e73dab Pin SHA256: TfUknRoG8EPFF/IfejfY9nW2CPiv9v5p3/1WM2e0urg= RSA 2048 bits (e 65537) / SHA1withRSA **WEAK SIGNATURE**
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	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3 **INSECURE**	Yes
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_SHA (`0x5`) **INSECURE**	128
TLS_RSA_WITH_AES_128_CBC_SHA (`0x2f`)	128
TLS_RSA_WITH_AES_256_CBC_SHA (`0x35`)	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (`0xa`)	112
TLS_RSA_WITH_AES_128_CBC_SHA256 (`0x3c`)	128

TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256

Handshake Simulation

Android 2.3.7 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Android 4.0.4	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Android 4.1.1	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Android 4.2.2	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Android 4.3	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Android 4.4.2	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Android 5.0.0	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Baidu Jan 2015	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
BingPreview Jan 2015	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Chrome 45 / OS X R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Firefox 31.3.0 ESR / Win 7	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Firefox 41 / OS X R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Googlebot Feb 2015	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 6 / XP No FS [1] No SNI [2]	SSL 3	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 7 / Vista	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 8 / XP No FS [1] No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 8-10 / Win 7 R	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 11 / Win 7 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 11 / Win 8.1 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
IE 10 / Win Phone 8.0	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
IE 11 / Win Phone 8.1 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
IE 11 / Win Phone 8.1 Update R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
IE 11 / Win 10 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Edge / Win 10 R	TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	No FS	128
Java 6u45 No SNI [2]	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Java 7u25	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Java 8u31	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
OpenSSL 0.9.8y	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
OpenSSL 1.0.1l R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
OpenSSL 1.0.2 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 5.1.9 / OS X 10.6.8	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 6 / iOS 6.0.1 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 6.0.4 / OS X 10.8.4 R	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 7 / iOS 7.1 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 7 / OS X 10.9 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 8 / iOS 8.4 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 8 / OS X 10.10 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 9 / iOS 9 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Safari 9 / OS X 10.11 R	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
Apple ATS 9 / iOS 9 R	Protocol or cipher suite mismatch			Fail[3]
Yahoo Slurp Jan 2015	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	No FS RC4	128
YandexBot Jan 2015	TLS 1.2	TLS_RSA_WITH_RC4_128_SHA (0x5)	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	**Supported DoS DANGER** (more info)
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info) SSL 3: 0x5, TLS 1.0: 0x5
POODLE (SSLv3)	No, mitigated (more info) SSL 3: 0x5
POODLE (TLS)	**Vulnerable INSECURE** (more info)
Downgrade attack prevention	**No, TLS_FALLBACK_SCSV not supported** (more info)
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** eastwestpersonal.com.ph
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 18:42:16 UTC
Test duration	334.914 seconds
HTTP status code	302
HTTP forwarding	**http://www.eastwestbanker.com PLAINTEXT**
HTTP server signature	-
Server hostname	www.eastwestpersonal.com.ph

SSL Report v1.20.28

Terms and Conditions