SSL Report: www.hiawatha-webserver.org (37.34.56.76)

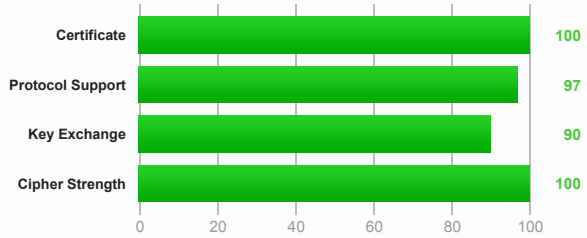
Assessed on: Tue Oct 30 17:38:52 UTC 2012 | Clear cache

Scan Another >>

Summary

Overall Rating

96



Documentation: SSL/TLS Deployment Best Practices and SSL Server Rating Guide 2009

This site works only in browsers with SNI support

Details

Certificate and Key Information

Common names	**www.hiawatha-webserver.org**
Alternative names	www.hiawatha-webserver.org hiawatha-webserver.org
Prefix handling	Both (with and without WWW)
Valid from	Sat Oct 27 00:00:00 UTC 2012
Valid until	Thu Oct 26 23:59:59 UTC 2017 (expires in 4 years and 11 months)
Key	RSA / 2048 bits
Signature algorithm	SHA1withRSA
Server Gated Cryptography	No
Weak key (Debian)	No
Issuer	PositiveSSL CA 2
Next Issuer	AddTrust External CA Root ***TRUSTED***
Chain length (size)	2 (2557 bytes)
Chain issues	None
Extended Validation	No
Revocation information	CRL, OCSP
Revocation status	Good (not revoked)
Trusted	**Yes**

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	No
SSL 3.0 **	No
SSL 2.0 **	No

(**) This site requires support for virtual SSL hosting, but SSL 2.0 and SSL 3.0 do not support this feature.

Cipher Suites (SSLv3+ suites in server-preferred order, then SSLv2 suites where used)

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits (p: 256, g: 256, Ys: 256)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits (p: 256, g: 256, Ys: 256)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits (p: 256, g: 256, Ys: 255)	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)		256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256

Protocol Details

Secure Renegotiation	**Supported, with client-initiated renegotiation disabled**
Insecure Renegotiation	Not supported
BEAST attack	**Not vulnerable**
Compression	No
Next Protocol Negotiation	No
Session resumption	Yes
Session tickets	No
OCSP stapling	No
Strict Transport Security	No
Requires client RI support	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	0x0304: 0x303, 0x0399: 0x303, 0x0499: fail

Miscellaneous

Test date	Tue Oct 30 17:37:43 UTC 2012
Test duration	68.809 seconds
Server signature	Hiawatha v8.6
Server hostname	leisink.org
PCI compliant	Yes
FIPS-ready	No

SSL Report v1.1.13 (Beta)