IIS Hardening Fact Sheet

v1.2.0

By Chris Campbell

The following hardened configuration is applied by IIS Fortify, a suite of scripts produced by the JADE Security Team.

HTTP Headers

Name	Value
cache-control	private, max-age=0, no-cache
Strict-Transport-Security	max-age=31536000; includeSubDomains
X-Content-Type-Options	nosniff
X-Download-Options,	noopen
X-Frame-Options	SAMEORIGIN
X-XSS-Protection	1; mode=block

Note: The above should be considered a minimum, base configuration for a server. Others (such as Content-Security-Policy) may also be added, and headers such as X-Frame-Options and cache-control may be adjusted according to individual application requirements.

More Information:
OWASP: https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Cryptography

Library:
Microsoft Schannel

Weak Ciphers Disabled:
NULL, DES and TDES, RC2 and RC4.

Insecure Protocols Disabled:
PCT, MPUH, SSL2.0 and SSL3.0.

Weak MAC's Disabled:
MD5 and SHA1.

Strong MAC's Enabled:

SHA256, SHA384 and SHA512.

Strong Ciphers Enabled:
AES128 and AES256.

Strong Key-Exchanges Enabled:
PKCS, DH and ECDH.

Secure Protocols Enabled:
TLS1.0, TLS1.1 and TLS1.2.

WDigest Algorithm:
3DES.

Cipher Suite:
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256

Note: Applicable to Server 2008+ only. Requires MS14-066 patch to be applied.
(*) : Applicable to Server 2012+ only.

More Information:
NIST Suite B: http://www.keylength.com/en/6/
Windows Compatibility:
http://blogs.msdn.com/b/kaushal/archive/2011/10/02/support-for-ssl-tls-protocols-on-windows.aspx