Here is the instructions for IIS SSL configuration.

More configurations can be found here: https://auditsquare.com/advisory/windows/iis-disable-weak-crypto

Microsoft IIS

To disable weak cipher suites in Microsoft IIS, you will need to make changes to the registry of the Windows OS it runs on.

Due to this, I have to warn you: Making changes to the registry could cause serious issues, so definitely make backups before proceeding!

If any of the registry keys I mention here don't exist, you can simply create them.

TLS Protocols

Disable TLS 1.0

Registry Path: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
Set DWORD value "Enabled" to 0
If Disabled By Default exists, set it to 1

Disable TLS 1.1 (unless you require it for legacy support)

Registry Path: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
Set DWORD value "Enabled" to 0
If Disabled By Default exists, set it to 1
If you require TLSv1.1, you don't need to change the current setting

Enable TLS 1.2 (If already enabled, don't need to change anything)

Registry Path: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server
Set DWORD value "Enabled" to 1
If Disabled By Default exists, set it to 0

Disable MD5 hashing

This is necessary as many of the weak hashing algorithms found used MD5 Hashing

Registry Path: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5
Set the DWORD value "Enabled" to 0.

Disable RC4

This is necessary as many of the weak hashing algorithms also used RC4 encryption.

Paths for all RC4 Ciphers:
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128

Set each one's DWORD value "Enabled" to 0.

Set Cipher Suites and their order

This one requires you to use the Group Policy Editor to change!

You will need to open gpedit.msc
Go to Computer Configuration ›› Administrative Templates ›› Network ›› SSL Configuration Settings ›› SSL Cipher Suite Order

Give it this value (They are separated by commas already):
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA