Recast

TLS Hardening

Last Modified on 04.16.26

TLS Hardening

By default, the HTTP.sys web server of the Microsoft Windows operating system allows the usage of insecure/obsolete protocols, ciphers, key exchange algorithms and hashes for maximum compatibility. As this allows a wide range of browsers to interact with the web server, it also exposes it to TLS attacks.

To prevent possible TLS attacks, we recommend you disable multiple obsolete and known insecure parts. SeeWikipedia TLS overview article to see a list of browsers and their support for TLS versions.

In October 2018, Apple, Google, Microsoft, and Mozilla jointly announced they would deprecate TLS 1.0 and 1.1 starting March 2020.
For TLS 1.2 support on different platforms and browsers, see Wikipedia TLS overview article.

Registry key example

The following registry code can be used to disable insecure/obsolete protocols, ciphers, key exchange algorithms and hashes.

> TLS Support
>
> The following registry example will disable TLS 1.0 and TLS 1.1. It can have an impact on the supported browsers that can connect to the webserver.

```
Windows Registry Editor Version 5.00

; Disable SSL 3.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

; Disable TLS 1.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001

; Disable TLS 1.1
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
"Enabled"=dword:00000000
"DisabledByDefault"=dword:00000001


; Disable weak ciphers
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128]
```

```
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]
"Enabled"=dword:00000000

; Disable weak key exchange algorithms
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS]
"Enabled"=dword:00000000


; Disable weak hashes
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]
"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA]
"Enabled"=dword:00000000

; Force server to not respond to renegotiation requests from client
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL]
"AllowInsecureRenegoClients"=dword:00000000
"AllowInsecureRenegoServers"=dword:00000000
"DisableRenegoOnServer"=dword:00000001
"UseScsvForTls"=dword:00000001
```