Schannel Information Disclosure Vulnerability

Issues:

Diffie-Hellman prime is less than 2048 bits
Remediation: Use OpenSSL or an SSL implementation of your choice to generate a new Diffie-Hellman group and key pair for your server greater than or equal to 2048 bits. Read more at weakdh.org.

Short Diffie-Hellman prime is very commonly used
Remediation: Use OpenSSL or an SSL implementation of your choice to generate a new Diffie-Hellman group for your server and make sure you have a strong TLS configuration, as documented at weakdh.org. To avoid a "WARN" rating on your new Diffie-Hellman group, create one at 2048 bits or greater.

Windows Server 2008,Windows Server 2008 R2,Windows Server 2012:

By default, Diffie-Hellman key exchange is enabled.

Workaround

The following workaround may be helpful in your situation:

- **Disable DHE cipher suites**

  Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

  1. Open Registry Editor.
  2. Access key exchange algorithm settings by navigating to the following registry location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms

3. Select the **Diffie-Hellman** sub key (if it does not exist, then create it).
4. Set the **Enabled** DWORD registry value to **0** (if it does not exist, then create it).
5. Exit Registry Editor.
6. Restart the web server for the changes to take effect.

How to undo the workaround.

1. Open Registry Editor.
2. Access key exchange algorithm settings by navigating to the following registry location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms

3. Select the **Diffie-Hellman** sub key.
4. Set the **Enabled** DWORD registry value to **1**.
5. Exit Registry Editor.
6. Restart the web server for the changes to take effect.

Impact of the workaround: Encrypted TLS sessions that rely on DHE keys will no longer function unless alternative failover options have been implemented.

Notes:

- When you disable any algorithm, you disallow all cipher suites that use that algorithm.
- See also Microsoft Knowledge Base article 245030: *How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll*

More to read:

https://technet.microsoft.com/en-us/library/security/ms15-055.aspx

http://robwillis.info/2015/10/hardening-ssl-tls-connections-on-windows-server-2008-r2-2012-r2/