# 网址：https://www.cnblogs.com/masahiro/p/15272066.html

# [Windows服务器中防御LOGJAM攻击与Sweet32攻击](https://www.cnblogs.com/masahiro/p/15272066.html)

LOGJAM 攻击是一个 SSL/TLS 漏洞，允许攻击者拦截易受攻击的客户端和服务器之间的 HTTPS 连接， 并强制它们使用“导出级”加密，然后可以对其进行解密或更改。发现网站支持 DH(E) 导出密码套件， 或使用小于 1024 位的 DH 素数或最大 1024 位的常用 DH 标准素数的非导出 DHE 密码套件时，会发出 此漏洞警报。

Sweet32 攻击是一个 SSL/TLS 漏洞，允许攻击者使用 64 位分组密码破坏 HTTPS 连接。

这两个攻击都指向了对低版本的 SSL/TLS与低版本的加密算法,在微软官方文档中也指出了禁用方案,下面是禁用的方法

一、禁用与启用SSL/TLS协议

在注册表中的 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols 路径下找到或建立相应协议版本的项

IMG_256

SSL 1.0

SSL 2.0

SSL 3.0

TLS 1.0

TLS 1.1

TLS 1.2

TLS 1.3

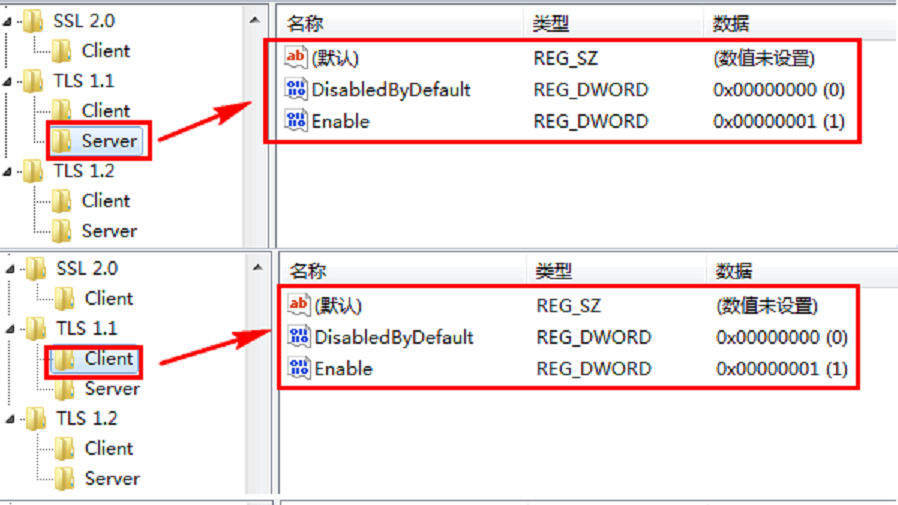
IMG_257

并在其下建立 Server 与 Client 项

在Server与Client中新建 DWORD（32位）值 如下

1 DisabledByDefault [Value = 1]2 Enable [Value = 0]

如下图：



二、禁用弱密码套件

 在注册表中的 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers 路径下找到或建立相应协议版本的项

IMG_259

RC4 128/128

Triple DES 168

RC2 128/128

RC4 64/128

RC4 56/128

RC2 56/128

DES 56/56

RC4 40/128

RC2 40/128

NULL

IMG_260

并在其中建立新建 DWORD（32位）值 如下

Enabled [Value = 0]

如果是Windows Vista及以上版本还可以使用以下下方法

通过在组策略对象编辑器中修改 SSL 密码套件顺序，您可以禁用 Windows Vista 及更高版本系统中的 RSA 密钥交换。

注意 安装此更新 (3046049) 可以防止公告中描述的漏洞。如果想使用先前禁用的任何密码，则之前已经实施了此变通方法的用户将需要执行以下步骤来撤消此变通方法。

若要禁用 RSA 密钥交换密码，您必须执行以下步骤来指定 Windows 应使用的密码：

1、在命令提示符下，键入 gpedit.msc，并按 Enter 键来启动“组策略对象编辑器”。

2、依次展开\*\*“计算机配置”、“管理模板”、“网络”\*\*，然后单击“SSL 配置设置”。

3、在“SSL 配置设置”下，单击“SSL 密码套件顺序”设置。

4、在“SSL 密码套件顺序”窗口中，单击“已启用”。

5、在\*\*选项:\*\*窗格中，双击以突出显示“SSL 密码套件”字段的全部内容，然后使用以下密码列表替换其内容：

IMG_261

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P256,

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384,

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256,

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P384,

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P256,

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384,

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256,

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384,

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384\_P384,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P256,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P384,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384\_P384,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256\_P256,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256\_P384,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P256,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P384,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P256,

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P384,

TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256,

TLS\_DHE\_DSS\_WITH\_AES\_128\_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

6、单击“确定”

7、关闭组策略对象编辑器。

注意：以上操作后需要重启计算机使其生效。

参考资料：

[Weak Diffie-Hellman and the Logjam Attack](https://weakdh.org/" \o "Weak Diffie-Hellman and the Logjam Attack" \t "C:/Users/Administrator/AppData/Local/Temp/CyberArticle/_blank)

[Guide to Deploying Diffie-Hellman for TLS](https://weakdh.org/sysadmin.html" \o "Guide to Deploying Diffie-Hellman for TLS" \t "C:/Users/Administrator/AppData/Local/Temp/CyberArticle/_blank)

[限制某些加密算法和协议在 Schannel.dll](https://docs.microsoft.com/zh-cn/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel" \o "限制某些加密算法和协议在 Schannel.dll" \t "C:/Users/Administrator/AppData/Local/Temp/CyberArticle/_blank)

[TLS/SSL (Schannel SSP) 中的密码套件](https://docs.microsoft.com/zh-cn/windows/win32/secauthn/cipher-suites-in-schannel?redirectedfrom=MSDN" \o "TLS/SSL (Schannel SSP) 中的密码套件" \t "C:/Users/Administrator/AppData/Local/Temp/CyberArticle/_blank)

[Schannel 中的漏洞可能允许绕过安全功能 (3046049)](https://docs.microsoft.com/zh-cn/security-updates/SecurityBulletins/2015/ms15-031?redirectedfrom=MSDN" \o "Schannel 中的漏洞可能允许绕过安全功能 (3046049)" \t "C:/Users/Administrator/AppData/Local/Temp/CyberArticle/_blank)

[Managing SSL/TLS Protocols and Cipher Suites for AD FS](https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/manage-ssl-protocols-in-ad-fs" \o "Managing SSL/TLS Protocols and Cipher Suites for AD FS" \t "C:/Users/Administrator/AppData/Local/Temp/CyberArticle/_blank)