

Windows10 推送的 KB3163018 补丁导致 TLS1.0 不可用

现象描述:

Windows 10 在 2016 年 6 月 14 日推送的 KB3163018 补丁，此补丁会导致部分 TLS1.0 不可用，主要影响的是 Edge 和 IE11 浏览器，对不依赖 IE 内核的浏览器没有影响。



无法显示此页

- 确保 Web 地址 https://172.16.2.94:16936 正确。
- 使用搜索引擎查找页面。
- 请过几分钟后刷新页面。

修复连接问题

问题原因:

windows10 在升级此补丁后，IE 和 Edge 禁用 TLS_DHE_RSA_WITH_AES_128_CBC_SHA，而 IE 或 Edge 浏览器向服务器发起 HTTPS 连接请求时，发送的密文族(ciphers suites)里却包含 TLS_DHE_RSA_WITH_AES_128_CBC_SHA，tomcat 旧的 HTTPS 配置方式会优先使用 TLS_DHE_RSA_WITH_AES_128_CBC_SHA，所以无法建立连接。

这么说吧，IE 在建立连接时，告诉服务器，我支持 A、B、C 加密算法，然后服务器说，用 A 算法加密，IE 通信层的程序又拒绝了 A 算法。导致无法建立连接。

我恨微软，1. 更新补丁没详细说明，2.程序没改全。

解决方案:

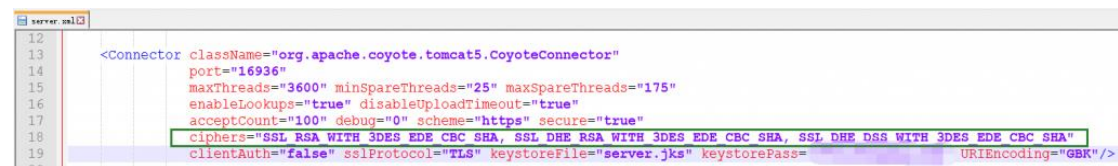
针对 tomcat 服务器:

1. 服务器是 tomcat 的, 修改配置文件 conf/server.xml 中 Connector 的属性

临时解决方案: 此方案优点, 配置很少, 而且兼容 IE6, IE8, IE9, IE10, IE11, 测试环境 win xp, win 7, win 10, 兼容 tomcat5, tomcat6 (测试确认了至少 3 个小版本), 兼容 JDK6 默认安装

```
ciphers="SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WIT  
H_AES_128_CBC_SHA"
```

配置位置如图 (图片供参考)



```
12  
13 <Connector className="org.apache.coyote.tomcat5.CoyoteConnector"  
14 port="16936"  
15 maxThreads="3600" minSpareThreads="25" maxSpareThreads="175"  
16 enableLookups="true" disableUploadTimeout="true"  
17 acceptCount="100" debug="0" scheme="https" secure="true"  
18 ciphers="SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"  
19 clientAuth="false" sslProtocol="TLS" keystoreFile="server.jks" keystorePass=  
URIEncoding="GBK"/>
```

说明:

SSL_RSA_WITH_RC4_128_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA 支持 IE6, IE8, IE9, IE10, IE11

TLS_RSA_WITH_AES_128_CBC_SHA 支持 IE9, IE10, IE11

建议解决方案: 升级 JDK 到 7 以上, 开启 TLS1.2, 并且将 tomcat 升级到最新版本。

2. 如果是 nginx, apache 之类的请参考 <https://cipherli.st/>

参考连接:

HTTPS 研究 (2) — 分解 HTTPS 连接建立过程

<http://www.jianshu.com/p/a766bbf31417>

apache Tomcat 配置 SSL(https)步骤

<http://www.cnblogs.com/qqzy168/archive/2013/08/03/3140252.html>

Tomcat6+JDK6 如何加固, 解决 Logjam attack

<http://rickqin.blog.51cto.com/blog/1096449/1682426>

参考资料:

https://developer.mozilla.org/en-US/Firefox/Releases/39/Site_Compatibility

<https://weakdh.org/> (Weak Diffie-Hellman and the Logjam Attack)

<https://weakdh.org/sysadmin.html> (各种服务器的 ciphers 配置方式)

<https://weakdh.org/logjam.html>

https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

JDK 6 支持的 ciphers 名称列表

<http://docs.oracle.com/javase/6/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider>

Java Cryptography Architecture Sun Providers Documentation

<http://docs.oracle.com/javase/6/docs/technotes/guides/security/SunProviders.html>

JavaTM Secure Socket Extension (JSSE) Reference Guide

<http://docs.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html>

Java Cryptography Architecture Standard Algorithm Name Documentation (jdk6 加密体系标准算法名)

<http://docs.oracle.com/javase/6/docs/technotes/guides/security/StandardNames.html>

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files (如果没有这个，不支持长度超过 128 的密码，比如 TLS_RSA_WITH_AES_128_CBC_SHA 中的 128)

<http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html>

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>

<http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>

配置方式： 下载后，解压缩 jce\local_policy.jar 和 jce\US_export_policy.jar 到 %JAVA_HOME%\jre\lib\security

TLS 漏洞参考：

关于 SSL/TLS 最新漏洞“受戒礼”初步报告

<http://www.freebuf.com/articles/network/62442.html>

关于 TLS 1.2 受到此前 SSL V3 “POODLE”漏洞攻击威胁的情况公告

<http://www.cnvd.org.cn/webinfo/show/3549>

POODLE 漏洞东山再起,影响 TLS 安全传输协议

<http://sec.chinabyte.com/157/13173657.shtml>

扩展阅读：

SSL 应用：今天截获,明天解密（[图片存档](#)）

<http://sec.chinabyte.com/298/12692298.shtml>

IE6, IE8, IE11 支持的 TLSv1.0 的 ciphers:

win10_ie11

Time	Source	Destination	Protocol	Length	Info
405 6.171103	192.168.1.100	172.16.2.46	TCP	54	42162 → 19401 [A
406 6.171385	192.168.1.100	172.16.2.46	TLSv1	180	Client Hello
407 6.172187	172.16.2.46	192.168.1.100	TCP	60	19401 → 42162 [A

Length: 121

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 117

Version: TLS 1.0 (0x0301)

Random

Session ID Length: 0

Cipher Suites Length: 28

Cipher Suites (14 suites)

- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
- Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
- Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
- Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)

Compression Methods Length: 1

winxp ie8

No.	Time	Source	Destination	Protocol	Length	Info
859	46.1920370	192.168.1.181	172.16.2.46	TCP	54	prusniarez > 19401
904	47.8520510	192.168.1.181	172.16.2.46	TCP	62	ibm-wrless-lan > 19401
905	47.8528130	172.16.2.46	192.168.1.181	TCP	62	19401 > ibm-wrless-lan
906	47.8528520	192.168.1.181	172.16.2.46	TCP	54	ibm-wrless-lan > 19401
907	47.8533360	192.168.1.181	172.16.2.46	TLSv1	156	Client Hello
908	47.8539880	172.16.2.46	192.168.1.181	TCP	60	19401 > ibm-wrless-lan

Transmission Control Protocol, Src Port: ibm-wrless-lan (1461), Dst Port: 19401 (19401)
 Secure Sockets Layer
 TLSv1 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 97
 Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 93
 Version: TLS 1.0 (0x0301)
 Random
 Session ID Length: 32
 Session ID: 577d992de6b5e9d295983fa537cbaf7eed88270742b8df39...
 Cipher suites Length: 22
 Cipher Suites (11 suites)
 Cipher suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
 Cipher suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
 Cipher suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
 Cipher suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
 Cipher suite: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
 Cipher suite: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x0062)
 Cipher suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
 Cipher suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
 Cipher suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
 Cipher suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
 Cipher suite: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x0063)
 Compression Methods Length: 1
 Compression Methods (1 method)

winxp ie6

No.	Time	Source	Destination	Protocol	Length	Info
202	8.85970400	192.168.1.182	172.16.2.46	TCP	94	cajo-discovery > 19401 [ACK]
203	8.84130000	192.168.1.182	172.16.2.46	TLSv1	124	Client Hello
204	8.84199500	172.16.2.46	192.168.1.182	TCP	60	19401 > cajo-discovery [ACK]
207	8.87606300	172.16.2.46	192.168.1.182	TLSv1	694	Server Hello, Certificate, S...
208	8.87700600	192.168.1.182	172.16.2.46	TLSv1	240	Client Key Exchange, Change C...

Frame 203: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface 0
 Ethernet II, Src: Vmware_d9:b3:37 (00:0c:29:d9:b3:37), Dst: Netgear_a2:67:a9 (c0:ff:d4:a2:67:a9)
 Internet Protocol Version 4, Src: 192.168.1.182 (192.168.1.182), Dst: 172.16.2.46 (172.16.2.46)
 Transmission Control Protocol, Src Port: cajo-discovery (1198), Dst Port: 19401 (19401), Seq: 1, Ack
 Secure Sockets Layer
 TLSv1 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 65
 Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 61
 Version: TLS 1.0 (0x0301)
 Random
 Session ID Length: 0
 Cipher suites Length: 22
 Cipher Suites (11 suites)
 Cipher suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
 Cipher suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
 Cipher suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
 Cipher suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
 Cipher suite: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
 Cipher suite: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x0062)
 Cipher suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
 Cipher suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
 Cipher suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
 Cipher suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
 Cipher suite: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x0063)
 Compression Methods Length: 1
 Compression Methods (1 method)

