SGC连接失败：使用不同的摘要提升并且导出密码

目录

简介

本文讨论在安全供应商Schannel.dll文件发生，用于微软互联网Information塞尔韦尔的问题(IIS)和微软Internet Explorer。此问题提交，当您连接到使用服务器装门的加密算法的站点(SGC)执行高加密，并且出口密码器套件使用一散列算法，当国内密码器套件使用别的时。在这种情况下，Schannel.dll文件偶尔地选择错误的算法，导致失败的连接。结果，网络客户端可能不能连接到使用SGC强加密的网站，当安全连接要求时。如果Internet服务器或网络客户端运行Microsoft产品，则连接可能发生故障。

Microsoft确认，当一加强密码器比出口密码器时使用一不同的摘要，连接可能发生故障。关于此问题的更多信息，参考的SGC连接可能从国内客户端失效 。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco内容服务(CSS)用安全套接字层SSL模块

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题

使用SGC在CSS SSL模块的加强cert，当客户端连接到站点通过SSL模块用56位浏览器时，浏览器建立在56的SSL连接而不是提高连接到128。

例如，请想象第一个客户端Hello协商rsa-export1024-with-rc4-56-sha密码器。根据命令如此的模块匹配在配置里(除非衡量密码器)，当加强发生时，模块很可能设法使用rsa-with-3des-ede-cbc-sha密码器。这两密码器文摘不配比，并且失败发生。不仅必须文摘配比，但是加密类型必须配比。

解决方案

凭用户代理列表，解决方案对此问题在此部分解释。

目前，客户有这些出口密码器：

- ssl服务器4
- ssl服务器4 VIP地址198.22.10.10
- ssl服务器4 rsakey CSSRsaKey4
- ssl服务器4 rsacert RsaCert4
- ssl服务器4密码器rsa-with-rc4-128-md5 198.22.10.10 20094
- ssl服务器4密码器rsa-with-rc4-128-sha 198.22.10.10 20094
- ssl服务器4密码器rsa-with-des-cbc-sha 198.22.10.10 20094
- ssl服务器4密码器rsa-with-3des-ede-cbc-sha 198.22.10.10 20094
- ssl服务器4密码器rsa-export1024-with-des-cbc-sha 198.22.10.10 20094
- ssl服务器4密码器rsa-export1024-with-rc4-56-sha 198.22.10.10 20094

要解决在本文讨论的问题，您必须选择一出口密码器支持(例如， rsa-export1024-with-rc4-56-sha)。这通常不是问题，因为，如果56位浏览器发送这些密码器之一，两个发送。您能当前配置其余您的强密码器，但是您必须衡量他们这样密码器(rsa-with-rc4-128-sha)有高权值。必须分配其他强密码器下强重要性和出口密码器最低的权重。这是什么的示例此配置看上去象(请注意出口密码器没有重要性，因为默认是1)：

注意： 在本例中，您有出口使用的密码器套件的两个选项。思科不能推荐哪个使用。您必须做出根据您的企业安全需求的决策。

解决方案 1

如果决定使用出口密码器(rsa-export1024-with-rc4-56-sha)，代理列表如下所示:

- ssl服务器5密码器rsa-with-rc4-128-sha 198.22.124.134 20094权重10
- ssl服务器5密码器rsa-with-rc4-128-md5 198.22.124.134 20094权重8
- ssl服务器5密码器rsa-with-des-cbc-sha 198.22.124.134 20094权重8
- ssl服务器5密码器rsa-with-3des-ede-cbc-sha 198.22.124.134 20094权重8
- ssl服务器5密码器rsa-export1024-with-rc4-56-sha 198.22.124.134 20094 weight1

解决方案 2

如果决定支持另一出口密码器(rsa-export1024-with-des-cbc-sha)，您的权重如下所示:

- ssl服务器5密码器rsa-with-des-cbc-sha 198.22.124.134 20094权重10
- ssl服务器5密码器rsa-with-rc4-128-sha 198.22.124.134 20094权重8
- ssl服务器5密码器rsa-with-rc4-128-md5 198.22.124.134 20094权重8
- ssl服务器5密码器rsa-with-3des-ede-cbc-sha 198.22.124.134 20094权重8
- ssl服务器5密码器rsa-export1024-with-des-cbc-sha 198.22.124.134 20094 weight1

相关信息

- 配置SSL流量通过CSS
- 技术支持 - Cisco Systems