Falhas da conexão SGC: Step-up e exporte resumos diferentes do uso das cifras

Índice

Introdução

Este documento endereça um problema que ocorra no arquivo do provedor de segurança Schannel.dll, que é usado em Microsoft Internet Information Server (IIS) e em Microsoft Internet explorer. Este problema apresenta quando você conecta a um local que use o server gated cryptography (SGC) para fazer a criptografia alta, e a série da cifra da exportação usa um algoritmo de hash quando a suite de cifra doméstica usar outro. Nesta situação, o arquivo Schannel.dll seleciona ocasionalmente o algoritmo errado, que conduz a uma falha na conexão. Em consequência, os clientes web podem não conectam aos sites que usam o SGC para a criptografia forte quando uma conexão segura é exigida. Se o servidor de Internet ou o cliente web estão executando produtos Microsoft, a seguir a conexão pode falhar.

Microsoft reconhece que quando uma cifra elevadora usa um resumo diferente do que a cifra da exportação, a conexão pode falhar. Para obter mais informações sobre deste problema, refira conexões SGC pode falhar dos clientes domésticos .

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Content Services (CSS) com módulo do Secure Socket Layer (SSL)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Problema

Com um CERT elevador SGC no módulo de CSS SSL, quando o cliente conecta a um local através do módulo SSL com um navegador 56-bit, o navegador estabelece uma conexão SSL em 56 um pouco do que intensificando a conexão ao 128.

Por exemplo, imagine que o primeiro hello do cliente negocia uma cifra do rsa-export1024-with-rc4-56-sha. Os fósforos do módulo baseados na ordem na configuração (a menos que as cifras são tornadas mais pesadas) assim quando o elevador ocorre, o módulo tentam provavelmente usar uma cifra de rsa-with-3des-ede-cbc-sha. Os resumos destas duas cifras não combinam, e a falha ocorre. Não somente devem os resumos combinar, MAS os tipos de criptografia devem combinar também.

Solução

Baseado na lista do proxy do cliente do exemplo, as soluções a este problema são explicadas nesta seção.

Atualmente, o cliente tem estas cifras da exportação:

- SSL-server 4
- endereço 198.22.10.10 vip do SSL-server 4
- rsakey CSSRsaKey4 do SSL-server 4
- rsacert RsaCert4 do SSL-server 4
- cifra rsa-with-rc4-128-md5 198.22.10.10 20094 do SSL-server 4
- cifra rsa-with-rc4-128-sha 198.22.10.10 20094 do SSL-server 4
- rsa-with-des-cbc-sha 198.22.10.10 20094 da cifra do SSL-server 4
- cifra rsa-with-3des-ede-cbc-sha 198.22.10.10 20094 do SSL-server 4
- cifra rsa-export1024-with-des-cbc-sha 198.22.10.10 20094 do SSL-server 4
- rsa-export1024-with-rc4-56-sha 198.22.10.10 20094 da cifra do SSL-server 4

Para resolver o problema discutido neste documento, você deve escolher uma cifra da exportação para apoiar (por exemplo, rsa-export1024-with-rc4-56-sha). Este não é geralmente um problema porque se um navegador 56-bit envia uma destas cifras, ambos são enviados. Você pode agora configurar o resto de suas cifras fortes, mas você deve torná-las mais pesadas tais que a cifra (rsa-with-rc4-128-sha) tem o peso o mais alto. As outras cifras fortes devem ser atribuídas os pesos os mais fortes seguintes, e a cifra da exportação o mais baixo peso. Está aqui uma amostra do que esta configuração olha como (nota que a cifra da exportação não tem nenhum peso porque o padrão é 1):

Nota: Neste exemplo, você tem duas opções em relação a que série da cifra da exportação a se usar. Cisco não pode recomendar qual usar-se. Você deve tomar uma decisão baseado em seus requisitos de segurança do negócio.

Solução 1

Se você decide usar a cifra da exportação (rsa-export1024-with-rc4-56-sha), a lista do proxy olha como esta:

- peso 10 da cifra rsa-with-rc4-128-sha 198.22.124.134 20094 do SSL-server 5
- peso 8 da cifra rsa-with-rc4-128-md5 198.22.124.134 20094 do SSL-server 5
- peso 8 de 198.22.124.134 20094 do rsa-with-des-cbc-sha da cifra do SSL-server 5
- peso 8 da cifra rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 do SSL-server 5
- peso 1 de 198.22.124.134 20094 do rsa-export1024-with-rc4-56-sha da cifra do SSL-server 5

Solução 2

Se você decide apoiar a outra cifra da exportação (rsa-export1024-with-des-cbc-sha), seus pesos olham como este:

- peso 10 de 198.22.124.134 20094 do rsa-with-des-cbc-sha da cifra do SSL-server 5
- peso 8 da cifra rsa-with-rc4-128-sha 198.22.124.134 20094 do SSL-server 5
- peso 8 da cifra rsa-with-rc4-128-md5 198.22.124.134 20094 do SSL-server 5
- peso 8 da cifra rsa-with-3des-ede-cbc-sha 198.22.124.134 20094 do SSL-server 5
- peso 1 da cifra rsa-export1024-with-des-cbc-sha 198.22.124.134 20094 do SSL-server 5

Informações Relacionadas

- Configurando o tráfego SSL com o CSS
- Suporte Técnico - Cisco Systems