# Pesquise defeitos edições do certificado para SSL VPN com CME

## Índice



## Introdução

Este documento descreve a metodologia para pesquisar defeitos o registro do telefone IP ao Gerenciador de Comunicações expresso (CME) através do secure sockets layer (SSL) VPN.

## Pré-requisitos

### Requisitos

Cisco recomenda que você tem uma compreensão básica de Certificados da Segurança, o pacote que captura a ferramenta, e o Gerenciador de Comunicações expresso.

### Componentes Utilizados

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

- Liberação expressa 8.6 do Gerenciador de Comunicações
- Liberação 8.5.3 do telefone IP de Cisco 7965

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.

## Pesquise defeitos edições do certificado

Há dois métodos para estabelecer SSL VPN entre um telefone IP no Internet e o CME dentro da rede corporativa.

- O CME é atrás de uma ferramenta de segurança adaptável de Cisco (ASA) que atue como o fim de cabeçalho de VPN. Nesta encenação, o CME e o ASA compartilham do mesmo certificado e o telefone IP negocia a instalação de segurança com o ASA.
- O CME é conectado ao Internet diretamente, e atua como o fim de cabeçalho de VPN. Negocia a instalação de segurança com o telefone IP diretamente.

Em ambas as encenações, estabelecer SSL VPN entre um telefone IP no Internet e o CME consiste em etapas similares:

1. O CME gerencie ou obtém um Security Certificate.
2. O CME “empurra” a mistura do certificado no formato de Base64 para o telefone através do arquivo de configuração que o telefone transfere do CME através do TFTP.
3. O telefone IP tenta entrar com o fim de cabeçalho de VPN e recebe o certificado através do protocolo do Transport Layer Security (TLS).
4. O telefone IP extrai a mistura do certificado e compara-a com a mistura que transferiu do CME mais cedo. Se a mistura combina, a seguir o telefone confia o fim de cabeçalho de VPN e continua com negociação mais adicional VPN.

## Verificar

A fim verificar que o CME empurrou a mistura para o telefone IP, verifique o arquivo de configuração que gerou para o telefone seguro. A fim simplificar esta etapa, você pode configurar o CME para gerar um arquivo de configuração pelo telefone e para armazená-lo no flash:

```
R009-3945-1(config-telephony)#cnf-file perphone
R009-3945-1(config-telephony)#cnf-file location flash:
```

A fim assegurar-se de que a configuração nova esteja gerada, recomenda-se recrear os arquivos de configuração:

```
R009-3945-1(config-telephony)#no create cnf-files
CNF files deleted
R009-3945-1(config-telephony)#create cnf-file
Creating CNF files
```

Depois que o arquivo de configuração correspondente nos indicadores do flash (para um ephone com o VPN-grupo configurado), você deve considerar este perto da extremidade do conteúdo de arquivo:

```
<vpnGroup>  <enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.201.160.201/SSLVPNphone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>fZ2xQHMBcWj/fSoNs5IkPbA2Pt8=</certHash1>
</credentials>
</vpnGroup>
```

O valor **certHash1** é a mistura do certificado. Quando o telefone IP recebe o certificado do fim de cabeçalho de VPN durante a instalação TLS, espera a mistura do certificado ser mesmo que o valor de hash armazenado. Se o telefone IP joga “um erro do certificado ruim”, poder-se-ia ser que os valores de hash não combinam.

A fim verificar, siga estas etapas para extrair o valor de hash da captura de pacote de informação recolhida entre o telefone IP e o fim de cabeçalho de VPN:

1. Encontre o pacote do dispositivo do fim de cabeçalho de VPN ao telefone IP que contém o certificado. Está tipicamente no pacote dos servidores hello TLS.
2. Expanda o conteúdo de pacote de informação e encontre o encabeçamento: **Secure Socket Layer > do registro TLS V1 camada > protocolo de handshake: Certificado > Certificados > certificado**.
3. Clicar com o botão direito o encabeçamento do certificado e exporte os valores para um arquivo .CER:
4. Abra o arquivo .CER, vá à aba dos detalhes, escolha Thumbprint, e escolha os valores. Os valores são a mistura encantam dentro o formato:
5. Em seguida, você converte a mistura de encanta a Base64 usando toda a ferramenta em linha da conversão Hex-to-Base64. O valor convertido pode ser comparado ao valor de hash no arquivo de configuração do telefone IP se não combinam, a seguir significa que a mistura recebida pelo telefone IP é de um certificado diferente do que o que é usado pelo fim de cabeçalho de VPN para o SSL.

# Informações Relacionadas

- Configurando o cliente VPN SSL para Telefones IP SCCP
- Suporte Técnico e Documentação - Cisco Systems

>