

As gotas RTCP Multistreaming de Cisco Expressway B2BUA refrescam pacotes durante a descryptografia em atendimentos do WebEx de Cisco

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Atendimentos afetados](#)

[Recomendação - Sistemas da elevação X8.7.x](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve uma edição que afete determinadas configurações do TelePresence com versões de software X8.7x do VCS de Cisco Expressway ou de Cisco.

Contribuído por Judith Andrews, escritor técnico de Cisco, com base em entradas dos engenheiros de TAC da Cisco.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Valor-limite immersive do IX5000 Series do Cisco TelePresence (todas as versões)
- Versão X8.7.x do server (VCS de Cisco) ou do Cisco Expressway de comunicação de vídeo do Cisco TelePresence e mais cedo
- Versões de servidor 4.3, 4.4(1.9), 4.2 ou mais adiantado do Cisco TelePresence
- Versões de servidor do Cisco TelePresence 4.4(1.16) ou mais atrasado

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.

Informações de Apoio

O mecanismo para a manutenção do estado de sessão em X8.7.x é susceptível às edições quando um alto número de SSRC ID esta presente em atendimentos cifrados. Estes incluem atendimentos dos valores-limite immersive que usam o Tip, ou dos valores-limite que se operam no modo do multistream. Esta edição foi resolvida pelo VCS/Expressway X8.8.x e mais tarde. Contudo, esta edição pode afetar os atendimentos cifrados onde uma do VCS/vias expressas em uma ou outra extremidade do trecho de chamada está ainda em X8.7.x quando a outro estiver em X8.8.x ou em mais tarde.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- [Cisco TelePresence TX9000 Series](#)
- Sistema do Cisco TelePresence (CTS)
- Outros pontos finais de vídeo

Atendimentos afetados

Chama dos sistemas immersive do TelePresence que se operam no modo TIP/MUX, ou dos outros sistemas do TelePresence que se operam no modo multistreaming.

Quando cifrado/decifrou pelo VCS de Cisco ou pelo Cisco Expressway X8.7.x.

Os sintomas são o vídeo pixelated que obtém progressivamente mais ruim. Então o valor-limite termina o atendimento (porque os problemas com descodificação de media recebidos conduzem à perda de pacotes percebida). Outros vídeo e questões de qualidade puderam igualmente ocorrer.

Com o server do Cisco TelePresence, este comportamento pôde provocar a edição:

- Versões 4.3 ou 4.4(1.9): compartilhar para mais do que a sessão refresca.
- Versões 4.2 ou anterior, ou 4.4(1.16) ou mais atrasado: começar e parar compartilhando de épocas múltiplas.

Nota: Esta edição não ocorre se qualquens um casos se aplicam: 1. A criptografia para/desde o VCS de Cisco/Cisco Expressway é desabilitada. 2. TIP/MUX é desabilitado (sistemas immersive). 3. Multistream é desabilitado. 4. Se o WebEx de Cisco é rechamada video involvida, e do WebEx (chame meu sistema de vídeo) está usado.

Recomendação - Sistemas da elevação X8.7.x

A infraestrutura da nuvem CMR (WebEx de Cisco) foi promovida de X8.7 para resolver a edição para os clientes que têm o VCS de Cisco ou os em-locais de Cisco Expressway X8.8.x. Isto significa que outros clientes que usam o híbrido CMR, que têm o VCS de Cisco/locais de Expressway X8.7.x, poderiam agora ver esta edição. Nós recomendamos fortemente que você promove seu VCS de Cisco/Expressway X8.7.x se você está usando valores-limite

multistream/immersive para atendimentos cifrados com a outra infraestrutura de Cisco, como a nuvem CMR ou Parceiros da terceira.

Informações Relacionadas

- [CSCvc47502](#)
- [CSCvc34689](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)