CRYPTO_INTERNAL_ERROR durante downloads seguros do Google Drive

Contents

Problema

Os arquivos criptografados do Google Sheets não são abertos quando acessados pelo Cisco Secure Access com a descriptografia de tráfego ativada. Os usuários encontram um CRYPTO_INTERNAL_ERROR durante downloads seguros do Google Drive. Esse problema ocorre especificamente quando a inspeção do Secure Web Gateway (SWG) está ativa, já que os cabeçalhos Range são ignorados durante o processo de descriptografia e inspeção, levando à interferência no mecanismo de download seguro do Google.

O problema afeta ambientes que usam a implementação RAVPN+ZTA e afeta o acesso a Google Sheets criptografados para grandes populações de usuários.

Ambiente

- Tecnologia: Cisco Secure Access (Suporte à solução)
- Subtecnologia: Acesso seguro
- Implementação: RAVPN+ZTA (VPN de acesso remoto + acesso zero confiável)
- Componente afetado: Perfil ZTA
- Domínios afetados: clients6.google.com e outros domínios relacionados ao Google Drive

Resolução

A resolução envolve a implementação de soluções temporárias enquanto monitora reparos

permanentes do lado do fornecedor.

As abordagens descritas nas próximas seções foram validadas para restaurar o acesso às Planilhas do Google criptografadas.

Opções Temporárias de Solução Alternativa

Opção 1: Desabilitar descriptografia de tráfego

Desabilite completamente a descriptografia de tráfego para os grupos ou políticas de usuários afetados. Isso restaura o acesso ao Google Sheets, mas remove todos os recursos de inspeção de segurança baseados em descriptografia.

Opção 2: Excluir domínios do Google Drive da descriptografia

Adicione domínios relacionados ao Google Drive à lista de não descriptografar na configuração de política do Secure Access:

- clients6.google.com
- Outros domínios relacionados ao Google Drive, conforme identificados na análise de tráfego

Essa abordagem mantém a descriptografia para outro tráfego enquanto permite que o Google Sheets funcione normalmente. No entanto, essa solução alternativa tem o compromisso de desabilitar a funcionalidade de bloqueio de upload do CASB Google Drive para os domínios excluídos.

Análise e monitoramento técnicos

A análise da Cisco confirmou que a inspeção do Secure Web Gateway ignora cabeçalhos Range para permitir uma verificação de segurança abrangente do conteúdo do arquivo. Esse comportamento interfere no processo de download seguro do Google Drive, que depende de

cabeçalhos Range para o fluxo de descriptografia adequado.

O Google reconheceu o problema e identificou que o comportamento do proxy (incluindo o Cisco Umbrella/proxy de rede) interfere nas solicitações de download seguro do Google Drive, removendo ou reescrevendo cabeçalhos Range. Isso força um download de arquivo completo que quebra o mecanismo de descriptografia do Google. O Google está desenvolvendo uma correção no lado do cliente, embora nenhuma hora estimada de chegada tenha sido fornecida.

Considerações de implementação

As empresas que implementam as soluções alternativas devem considerar as implicações de segurança:

- Avalie o risco de excluir domínios do Google Drive da inspeção de descriptografia.
- Reveja as políticas CASB que podem ser afetadas pelas exclusões de domínio.
- Documente a natureza temporária da solução alternativa para revisões futuras de políticas.
- Monitore atualizações do Google com relação ao desenvolvimento de correções no lado do cliente.

Causa

A causa raiz é um problema de compatibilidade entre o comportamento de inspeção do Cisco Secure Access SWG e o mecanismo de download seguro do Google Drive.

Especificamente:

A inspeção do Cisco Secure Web Gateway ignora cabeçalhos Range durante o processo de descriptografia e verificação de segurança para garantir a análise completa do arquivo. No entanto, o acesso a arquivos criptografados do Google Drive depende de cabeçalhos Range para lidar adequadamente com o fluxo de descriptografia para downloads seguros. Quando esses cabeçalhos são removidos ou modificados durante o processo de inspeção de proxy, a descriptografia do cliente do Google falha, resultando em CRYPTO_INTERNAL_ERROR.

Isso representa uma incompatibilidade fundamental entre os requisitos de inspeção de segurança

(varredura de arquivos completa) e o mecanismo de entrega de arquivos criptografados do Google (downloads seguros baseados em intervalo).

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.