

Entender a Fixação de Chave Pública e a Fixação de Certificado no Umbrella

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Compatibilidade com o Umbrella SWG](#)

[Outros Aplicativos de Fixação de Certificado](#)

Introdução

Este documento descreve a fixação de certificado e a fixação de chave pública no Cisco Umbrella.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

A fixação de certificado é um mecanismo de segurança da Internet que permite que os aplicativos resistam à representação contra servidores HTTPS usando certificados digitais emitidos incorretamente ou de outra forma fraudulentos. Ele faz isso associando um servidor a um conjunto definido de chaves públicas, que podem ser as únicas confiáveis para conexões com esse servidor. Há duas técnicas para a Fixação de Certificado:

- A Fixação de Chave Pública (PKP RFC7469) é um mecanismo agora obsoleto para acionar

a fixação de certificado em navegadores da Web. Os certificados fixados são enviados para o navegador usando cabeçalhos HTTP.

- A Fixação de Certificado Estático é onde um aplicativo é codificado para esperar certificados específicos ou autoridades de certificado. Alguns aplicativos móveis/de desktop usam um mecanismo de fixação de certificado estático para segurança adicional.

Quando esses aplicativos da Web são intermediados por proxy pelo Umbrella, a chave pública fornecida pelo Umbrella não corresponde, o que faz com que o aplicativo feche a conexão HTTPS. A fixação de certificado geralmente se aplica apenas a aplicativos móveis/desktop, pois o suporte a PKP foi removido por navegadores da Web modernos.

Compatibilidade com o Umbrella SWG

O Umbrella ignora URLs conhecidas da Descriptografia SSL para resolver problemas de fixação de certificado em determinadas circunstâncias. A Tabela 1 inclui aplicativos que foram ignorados globalmente para todos os clientes do Umbrella. A Tabela 1 também inclui outros aplicativos que costumavam usar a fixação de certificado no momento da gravação. Se você estiver usando qualquer um desses aplicativos, poderá usar os métodos descritos posteriormente, pelos motivos apresentados, para ignorar o aplicativo da inspeção HTTPS. A Tabela 2 fornece mais detalhes para os serviços de aplicativos cobertos na Tabela 1.

Outros Aplicativos de Fixação de Certificado

Os aplicativos podem ser ignorados em uma base por cliente (por política) para resolver problemas de fixação de certificado usando o recurso [decodificação seletiva](#) do Umbrella. Estas exceções podem ser facilmente implementadas com base no domínio, no nome do aplicativo ou na categoria; O Umbrella SWG inclui uma grande biblioteca de aplicativos em nosso banco de dados de aplicativos.

Na maioria dos casos, a decisão de ignorar ou não o aplicativo é do administrador de TI. Adicionar uma exceção de descriptografia é uma compensação de segurança porque impede a inspeção de segurança/arquivo do conteúdo da Web. Essa é uma decisão individual, dependendo do tipo de aplicativo e da necessidade comercial. Por exemplo, se o problema de fixação do certificado afetar apenas um aplicativo móvel/desktop, o administrador pode optar por adicionar uma exceção para fazer o aplicativo móvel funcionar ou pode preferir pedir que os usuários usem a versão da Web do aplicativo.

Esta é uma tabela de aplicativos que são ignorados globalmente para clientes Umbrella e nenhuma ação é necessária ou conhecida para usar a fixação de certificado no momento da escrita e não ignorada pelo Umbrella por padrão. Se você estiver usando os aplicativos que não são ignorados por padrão, considere usar os métodos descritos acima, pelos motivos fornecidos, para ignorar o aplicativo da inspeção HTTPS.

Tabela 1 - Aplicativos que podem usar fixação de certificado

Nome do aplicativo	Cobertura do Cisco Umbrella
Serviços da Adobe	Ignorado globalmente pelos clientes da Umbrella
Airbnb	Suportado pelo Controle de Aplicativos
Amazon Alexa	Suportado pelo Controle de Aplicativos
Unidade Amazon	Suportado pelo Controle de Aplicativos
Amazon Kindle	Suportado pelo Controle de Aplicativos
Espaços de trabalho da Amazon	Suportado pelo Controle de Aplicativos
Amplitude	Ignorado globalmente pelos clientes da Umbrella
Dinâmica do Aplicativo	Ignorado globalmente pelos clientes da Umbrella
Apple iMessage	Suportado pelo Controle de Aplicativos
Apple Mail	Suportado pelo Controle de Aplicativos
Apple Services (consulte a tabela 2 para obter mais detalhes)	Ignorado globalmente pelos clientes da Umbrella
Cisco Services (consulte a tabela 2 para obter mais detalhes)	Ignorado globalmente pelos clientes da Umbrella
Espaço de trabalho Citrix	Suportado pelo Controle de Aplicativos
Crashlytics	Ignorado globalmente pelos clientes da Umbrella

Falcão CrowdStrike	Suportado pelo Controle de Aplicativos
Diligent.com	Suportado pelo Controle de Aplicativos
Bate-papo Discórdia	Ignorado globalmente pelos clientes da Umbrella
Nuvem do Contrato DocuSign	Suportado pelo Controle de Aplicativos
DropBox	Suportado pelo Controle de Aplicativos
Backup em nuvem Druva	Suportado pelo Controle de Aplicativos
Conexão Egnyte	Suportado pelo Controle de Aplicativos
Evernote	Suportado pelo Controle de Aplicativos
Messenger do Facebook	Suportado pelo Controle de Aplicativos
Facebook	Suportado pelo Controle de Aplicativos
E-mail de arquivo	Suportado pelo Controle de Aplicativos
Quadrangular	Suportado pelo Controle de Aplicativos
Giphy	Ignorado globalmente pelos clientes da Umbrella
GitHub	Suportado pelo Controle de Aplicativos
Google Drive	Suportado pelo Controle de Aplicativos
Google Play Store	Suportado pelo Controle de Aplicativos
Google Services (consulte a tabela 2 para obter mais detalhes)	Ignorado globalmente pelos clientes da Umbrella

Espaço de trabalho do Google	Suportado pelo Controle de Aplicativos
IrParaReunião	Suportado pelo Controle de Aplicativos
Máquina Hype	Suportado pelo Controle de Aplicativos
InstagramName	Suportado pelo Controle de Aplicativos
LogMein Pro	Suportado pelo Controle de Aplicativos
Microsoft Defender para endpoint	Suportado pelo Controle de Aplicativos
Microsoft Intune	Suportado pelo Controle de Aplicativos
Serviços Microsoft (consulte a tabela 2 para obter mais detalhes)	Ignorado globalmente pelos clientes da Umbrella
Microsoft Xbox Live	Suportado pelo Controle de Aplicativos
Netflix	Suportado pelo Controle de Aplicativos
OpenDrive	Suportado pelo Controle de Aplicativos
PayPal	Suportado pelo Controle de Aplicativos
Identidade PingOne	Suportado pelo Controle de Aplicativos
Serviços de unidade de rack / nuvem	Ignorado globalmente pelos clientes da Umbrella
CRM Salesforce	Suportado pelo Controle de Aplicativos
Segmento	Ignorado globalmente pelos clientes da Umbrella
Plataforma de Sinal	Suportado pelo Controle de Aplicativos

Skype para empresas	Suportado pelo Controle de Aplicativos
Snapchat	Suportado pelo Controle de Aplicativos
Soundcloud	Suportado pelo Controle de Aplicativos
Carvalho-aranha	Suportado pelo Controle de Aplicativos
Spotify	Suportado pelo Controle de Aplicativos
VisualizadorEquipe	Suportado pelo Controle de Aplicativos
TikTokName	Suportado pelo Controle de Aplicativos
Todoista	Suportado pelo Controle de Aplicativos
Twitter	Suportado pelo Controle de Aplicativos
Vimeo	Suportado pelo Controle de Aplicativos
HCM de dia útil	Suportado pelo Controle de Aplicativos
Reuniões com zoom	Ignorado globalmente pelos clientes da Umbrella

Tabela 2 - Detalhes para Serviços ignorados globalmente como mostrado na tabela 1

Serviços da Apple	• Verificação do Portal Cativo da Apple • Apple iTunes e App Store • Serviços adicionais da plataforma Apple
Serviços Cisco	• Serviços Cisco Umbrella e OpenDNS • Equipes Cisco Webex e Webex • WebUI do Cisco Cloud Email Security • Serviço de endpoint da AMP • Segurança Duo 2FA

Serviços do Google	• Google Hangouts • Mensagens do Google na Web • Serviços adicionais da plataforma Google
Serviços da Microsoft	• Indicador de Status de Conectividade de Rede da Microsoft • Atualização do Windows • Serviço de tradução do Windows • Serviços adicionais de plataforma Microsoft/Windows

Para obter ajuda adicional, consulte Solução de problemas de aplicativos que não são navegadores ou [entre em contato com o suporte Umbrella](#). Os pedidos podem ser considerados para adição à nossa lista global de desvio depois de terem sido revisados pela equipe de Engenharia.

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.