Comprendre l'épinglage de clé publique et l'épinglage de certificat dans Umbrella

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Aperçu](#)

[Compatibilité avec Umbrella SWG](#)

[Autres applications d'épinglage de certificat](#)

Introduction

Ce document décrit l'épinglage de certificat et l'épinglage de clé publique dans Cisco Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

L'épinglage de certificat est un mécanisme de sécurité Internet qui permet aux applications de résister à l'usurpation d'identité contre des serveurs HTTPS en utilisant des certificats numériques mal émis ou frauduleux. Pour ce faire, il associe un serveur à un ensemble défini de clés publiques, qui peuvent être les seules fiables pour les connexions à ce serveur. Il existe deux techniques pour l'épinglage de certificat :

- L'épinglage de clé publique (PKP RFC7469) est un mécanisme désormais obsolète pour déclencher l'épinglage de certificat dans les navigateurs Web. Les certificats épinglés sont envoyés au navigateur à l'aide d'en-têtes HTTP.

- L'épinglement de certificat statique est l'emplacement où une application est codée en dur pour attendre des certificats ou des autorités de certification spécifiques. Certaines applications de bureau/mobiles utilisent un mécanisme d'épinglement de certificat statique pour une sécurité supplémentaire.

Lorsque ces applications Web sont mises en proxy par Umbrella, la clé publique fournie par Umbrella ne correspond pas, ce qui entraîne la fermeture de la connexion HTTPS par l'application. L'épinglement de certificat s'applique généralement uniquement aux applications de bureau/mobiles, car la prise en charge de PKP a été supprimée par les navigateurs Web modernes.

Compatibilité avec Umbrella SWG

Umbrella contourne les URL connues du décodage SSL pour résoudre les problèmes d'épinglement de certificat dans certaines circonstances. Le tableau 1 inclut les applications qui ont été contournées globalement pour tous les clients Umbrella. Le tableau 1 inclut également d'autres applications connues pour utiliser l'épinglement de certificat au moment de la rédaction. Si vous utilisez l'une de ces applications, vous pouvez envisager d'utiliser les méthodes décrites plus loin, pour les raisons indiquées, pour contourner l'application de l'inspection HTTPS. Le tableau 2 fournit plus de détails sur les services d'application traités dans le tableau 1.

Autres applications d'épinglement de certificat

Les applications peuvent être contournées sur une base par client (par politique) pour résoudre les problèmes d'épinglement de certificat à l'aide de la fonctionnalité de [décodage sélectif](#) d'Umbrella. Ces exceptions peuvent être mises en oeuvre facilement en fonction du domaine, du nom de l'application ou de la catégorie ; Umbrella SWG inclut une grande bibliothèque d'applications dans notre base de données d'applications.

Dans la plupart des cas, la décision de contourner l'application incombe à l'administrateur informatique. L'ajout d'une exception de déchiffrement est un compromis de sécurité car il empêche l'inspection de sécurité/fichier du contenu Web. Il s'agit d'une décision individuelle en fonction du type d'application et des besoins de l'entreprise. Par exemple, si le problème d'épinglement de certificat affecte uniquement une application mobile/de bureau, l'administrateur peut choisir d'ajouter une exception pour que l'application mobile fonctionne ou préférer demander aux utilisateurs d'utiliser la version Web de l'application.

Il s'agit d'un tableau d'applications qui sont soit contournées globalement pour les clients Umbrella et aucune action n'est requise ou connue pour utiliser l'épinglement de certificat au moment de la rédaction et non contournées par Umbrella par défaut. Si vous utilisez les applications qui ne sont pas contournées par défaut, vous pouvez envisager d'utiliser les méthodes décrites ci-dessus, pour les raisons indiquées, pour contourner l'application de l'inspection HTTPS.

Tableau 1 - Applications pouvant utiliser l'épinglement de certificat

Nom de l'application	Couverture Cisco Umbrella
Services Adobe	Contourné dans le monde entier pour les clients Umbrella
Airbnb	Pris en charge par Application Control
Amazon Alexa	Pris en charge par Application Control
Lecteur Amazon	Pris en charge par Application Control
Amazon Kindle	Pris en charge par Application Control
Espaces de travail Amazon	Pris en charge par Application Control
Amplitude	Contourné dans le monde entier pour les clients Umbrella
Dynamique des applications	Contourné dans le monde entier pour les clients Umbrella
Apple iMessage	Pris en charge par Application Control
Apple Mail	Pris en charge par Application Control
Services Apple (voir le tableau 2 pour plus de détails)	Contourné dans le monde entier pour les clients Umbrella
Services Cisco (voir le tableau 2 pour plus de détails)	Contourné dans le monde entier pour les clients Umbrella
Citrix Workspace	Pris en charge par Application Control
Crashlytics	Contourné dans le monde entier pour les clients Umbrella

Faucon FrappeFoule	Pris en charge par Application Control
Diligent.com	Pris en charge par Application Control
Discorde Chat	Contourné dans le monde entier pour les clients Umbrella
Cloud d'accord DocuSign	Pris en charge par Application Control
DropBox	Pris en charge par Application Control
Druva Cloud Backup	Pris en charge par Application Control
Engyte Connect	Pris en charge par Application Control
Evernote	Pris en charge par Application Control
Facebook Messenger	Pris en charge par Application Control
Facebook	Pris en charge par Application Control
Filemail	Pris en charge par Application Control
Quadratique	Pris en charge par Application Control
Giphy	Contourné dans le monde entier pour les clients Umbrella
GitHub	Pris en charge par Application Control
Google Drive	Pris en charge par Application Control
Google Play Store	Pris en charge par Application Control
Google Services (voir tableau 2 pour plus de détails)	Contourné dans le monde entier pour les clients Umbrella

Espace de travail Google	Pris en charge par Application Control
AtteindreTéléconférence	Pris en charge par Application Control
Machine Hype	Pris en charge par Application Control
Instagram	Pris en charge par Application Control
LogMein Pro	Pris en charge par Application Control
Microsoft Defender pour les terminaux	Pris en charge par Application Control
Microsoft Intune	Pris en charge par Application Control
Services Microsoft (voir le tableau 2 pour plus de détails)	Contourné dans le monde entier pour les clients Umbrella
Microsoft Xbox Live	Pris en charge par Application Control
Netflix	Pris en charge par Application Control
OpenDrive	Pris en charge par Application Control
PayPal	Pris en charge par Application Control
Identité PingOne	Pris en charge par Application Control
Services d'espace rack/disque cloud	Contourné dans le monde entier pour les clients Umbrella
Salesforce CRM	Pris en charge par Application Control
Segment	Contourné dans le monde entier pour les clients Umbrella
Plate-Forme De Signalisation	Pris en charge par Application Control

Skype Entreprise	Pris en charge par Application Control
Snapchat	Pris en charge par Application Control
Nuage sonore	Pris en charge par Application Control
Chêne-Araignée	Pris en charge par Application Control
Spotifier	Pris en charge par Application Control
VisionneuseÉquipe	Pris en charge par Application Control
TikTok	Pris en charge par Application Control
Todoïste	Pris en charge par Application Control
Twitter	Pris en charge par Application Control
Vimeo	Pris en charge par Application Control
HCM Workday	Pris en charge par Application Control
Zoom sur les téléconférences	Contourné dans le monde entier pour les clients Umbrella

Tableau 2 - Détails pour Services ignorés globalement, comme indiqué dans le tableau 1

Services Apple	<ul style="list-style-type: none"> • Contrôle du portail captif Apple • Apple iTunes et App Store • Services de plateforme Apple supplémentaires
Services Cisco	<ul style="list-style-type: none"> • Services Cisco Umbrella et OpenDNS • Équipes Cisco Webex et Webex • Interface Web de sécurité de messagerie cloud Cisco • Service de terminaux AMP • Sécurité Duo 2FA

Services Google	<ul style="list-style-type: none">• Google Hangouts• Messages Google sur le Web• Services de plateforme Google supplémentaires
Services Microsoft	<ul style="list-style-type: none">• Indicateur d'état de connectivité réseau Microsoft• Windows Update• service de traduction Windows• Services de plate-forme Microsoft/Windows supplémentaires

Pour obtenir de l'aide supplémentaire, consultez la rubrique Dépannage d'applications sans navigateur ou [contactez l'assistance Umbrella](#). Les applications peuvent être considérées pour être ajoutées à notre liste de contournement globale après avoir été examinées par l'équipe d'ingénierie.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.