

WSA nouvel certificat racine paquet mise à jour en avril 2017 de confiance

Contenu

[Introduction](#)

[Fond](#)

[Description de mise à jour](#)

[Que fait ce moyen pour des utilisateurs WSA ?](#)

Introduction

Ce document décrit des détails au sujet de la mise à jour d'avril 2017 des paquets et des effets de confiance par Cisco de racine sur l'appliance de sécurité Web de Cisco (WSA).

Fond

Dans l'effort de garder le degré de sécurité de nos Produits au de plus haut niveau ; L'équipe cryptographique de services de Cisco est heureuse d'annoncer la release de la prochaine itération des paquets de racine de confiance par Cisco. Cette modification exercera également un effet sur WSA. Les paquets seront automatiquement mis à jour sur toutes les versions prises en charge de Cisco AsyncOS pour le Web, et il n'y a aucune action requise des administrateurs WSA.

Description de mise à jour

Ces paquets reflètent les dernières mises à jour aux paquets ont dérivé les mémoires de confiance d'amont à partir de novembre 2016 de racine.

Les modifications les plus importantes à Cisco ont fait confiance à des paquets de racine pour noter :

- Conformément à la décision des mémoires importantes de confiance ([Google](#), [Apple](#), [Mozilla](#)) de les retirer, nouveau Cisco a fait confiance que des paquets de racine **ne contiennent plus des** racines de **WoSign/StartCom**. Au cas où ils resoumettraient de nouvelles racines aux mémoires en amont de racine, nous revisiterons la décision de les retirer des paquets de confiance.
- Nouveau Cisco enracinent CA 2099 a été ajouté à tous les paquets pour prendre en charge les nouveaux jeux de puces ACT2.
- La vieille racine de Verisign a été au centre paquet remplacé avec la racine plus nouvelle cette enchaîne correctement des Certificats de mPKI de Verisign.
- La racine CA X1 DST a été retirée du principal paquet seulement, car Cisco n'émet plus des racines de cette chaîne.

Que fait ce moyen pour des utilisateurs WSA ?

- Cisco WSA téléchargera de nouveaux paquets de certificat racine utilisant notre processus d'update. Aucune action n'est nécessaire des administrateurs WSA
- Si WSA est configuré pour utiliser le déchiffrement, demande vers les sites qui ont des Certificats SSL signés par **WoSign/StartCom**, sera par défaut relâché par WSA, car les Certificats CA de racine de ce constructeur pas sont de confiance par WSA après la mise à jour.
- Alternativement, WSA appliquera l'action configurée dans le proxy HTTPS - > certificat non valide manipulant - > autorité non reconnue/émetteur de racine. Cette action est BAISSÉ par défaut, et Cisco recommande de ne pas changer l'action non reconnue par défaut d'autorité de racine.