Nueva actualización del conjunto del certificado de la Raíz confiable WSA - Abril de 2017

Contenido

Introducción

Este documento describe los detalles sobre la actualización de abril de 2017 de los conjuntos de la Raíz confiable de Cisco y sus efectos sobre el dispositivo de seguridad de la red de Cisco (WSA).

Antecedentes

En esfuerzo para guardar la Seguridad de nuestros Productos en el del más alto nivel; El equipo criptográfico de los servicios de Cisco está satisfecho anunciar la versión de la siguiente iteración de los conjuntos de la Raíz confiable de Cisco. Este cambio tendrá un efecto sobre WSA. Pondrán al día a los conjuntos automáticamente en todas las versiones admitidas de Cisco AsyncOS para la red, y no hay acciones necesarias de los administradores WSA.

Descripción de la actualización

Estos conjuntos reflejan las últimas actualizaciones a los conjuntos derivados de los almacenes por aguas arriba en noviembre 2016 de la Raíz confiable.

Los cambios más importantes a la Raíz confiable de Cisco lían para observar:

- Conforme a la decisión de los almacenes importantes de la confianza (Google, Apple, Mozilla) para quitarlos, los nuevos conjuntos de la Raíz confiable de Cisco contienen no más las raíces de WoSign/StartCom. Si resometen las nuevas raíces a los Almacenes raíz por aguas arriba, revisitaremos la decisión para quitarlos de los conjuntos de la confianza.
- Nuevo Cisco raíz CA 2099 se ha agregado a todos los conjuntos para soportar el nuevo chipsets ACT2.
- La vieja raíz de Verisign se ha substituido en el conjunto de la base por la más nueva raíz esa encadena correctamente los Certificados del mPKI de Verisign.
- El DST raíz CA X1 se ha quitado del conjunto de la base solamente, pues Cisco publica no más las raíces de este encadenamiento.

¿Qué hace este medio para los usuarios WSA?

- Cisco WSA descarga a los nuevos conjuntos del certificado raíz que utiliza nuestro proceso actualización. No hay acción necesaria de los administradores WSA.
- Si WSA se configura para utilizar el desciframiento, pide hacia los sitios que tienen Certificados SSL firmados por **WoSign/StartCom**, por abandono será caído por WSA, pues raíz CA los Certificados de este vendedor no serán confiados en por WSA después de la actualización.
- Alternativamente, WSA aplicará la acción configurada en el **proxy HTTPS > certificado inválido que dirige > autoridad desconocida/emisor de la raíz.** Esta acción es DESCENSO por abandono, y Cisco recomienda no cambiar la acción desconocida predeterminada de la autoridad de la raíz.