¿Por qué WSA elimina la información CRL de los Certificados generados mientras que desencripta el tráfico HTTPS?

Contenido

[Preguntas](#)
[Entorno](#)
[Síntomas](#)

Preguntas

1. ¿Por qué hace la información de la tira CRL del dispositivo de seguridad de la red de Cisco (WSA) de los Certificados generados mientras que desencripta el tráfico HTTPS?
2. Al generar un certificado de servidor del “spoofed” durante el descifrado SSL, el WSA elimina el Listas de revocación de certificados (CRL) del certificado original. ¿Por qué se hace esto?

Entorno

WSA cualquier versión, proxy HTTPS y descifrado SSL habilitados.

Síntomas

La información CRL en el certificado de servidor original está no más presente en el certificado generado mientras que el tráfico HTTPS que desencripta en WSA, y los clientes no pueden confirmar así si se ha revocado el certificado.

El WSA elimina la información CRL porque es no más válido para el certificado generado. La explicación implica una comprensión de cómo los CRL trabajan.

Un Certificate Authority (CA) puede mantener opcionalmente una lista de Certificados que considere no más válidos, llamado un Lista de revocación de certificados (CRL), o de CRL. Un certificado se puede revocar por una variedad de razones - el CA puede determinar que era la entidad que pidió el certificado no es quién él dijo ellos, o la clave privada se asoció al certificado se puede señalar robado. Los clientes que están validando una identidad del servidor Web basada en un certificado de servidor firmado pueden consultar el CRL para confirmar que el certificado no se ha revocado.

Un CRL contiene una lista de Certificados que han sido revocados por CA determinado y esa lista entonces es firmada por los Certificados revocados CA es identificada por el número de serie. Un

cliente puede extraer este CRL y después confirmar que el certificado de servidor no está enumerado en el CRL. El URL para descargar el CRL se incluye generalmente como campo en el certificado. Como manera práctica, la mayoría de los clientes no validan los Certificados contra un CRL.

Cuando el WSA está desencriptando el tráfico HTTPS o SSL, hace esto generando un nuevo certificado de servidor y firmándolo con su propio CA interno **(certificado cargado o generado bajo sección del proxy HTTPS)**.

Si el WSA no eliminara la información **CRL**, después un cliente que quiso validar el CRL encontraría que el **certificado** y el **CRL son firmados por diversas autoridades de certificación**, e ignorar el CRL o señalar un error por medio de una bandera. Además, en algunas circunstancias, el WSA cambiará el número de serie en el certificado generado para ser diferente que el número de serie en el certificado original. Esto significa que, incluso si un cliente ignoró la diferencia en CA entre el CRL y el certificado WSA-generado, la información del número de serie no sería válida.

La mejor manera de abordar el problema está para que el WSA valide el CRL sí mismo, en nombre el cliente y después excluya la información CRL del certificado. WSA no es capaz de hacer esto hoy.

En las versiones 7.7 de AsyncOS y arriba:

Comenzando con la versión 7.7 de AsyncOS, el WSA soporta el protocolo en línea del estado de certificación (**OCSP**) que es una alternativa al CRL.

Cuando está habilitado, OCSP proporciona la capacidad de obtener el estado de anulación de un certificado digital X.509.