Por que WSA descasca a informação CRL dos Certificados gerados ao decifrar o tráfego HTTPS?

Índice

Perguntas

1. Por que faz a informação da tira CRL da ferramenta de segurança da Web de Cisco (WSA) dos Certificados gerados ao decifrar o tráfego HTTPS?
2. Ao gerar um certificado de servidor “falsificado” durante a decriptografia de SSL, o WSA descasca o Certificate Revocation List (CRL) do certificado original. Por que isto é feito?

Ambiente

WSA alguma versão, proxy HTTPS e decriptografia de SSL permitidos.

Sintomas

A informação CRL no certificado de servidor original está já não atual no certificado gerado quando o tráfego de descriptografia HTTPS em WSA, e assim os clientes não puderem confirmar se o certificado esteve revogado.

O WSA descasca a informação CRL porque é já não válido para o certificado gerado. A explicação envolve uma compreensão de como os CRL trabalham.

Um Certificate Authority (CA) pode opcionalmente manter uma lista de Certificados que considera já não válidos, chamado uma lista de revogação de certificado, ou de CRL. Um certificado pode ser revogado por vários motivos - CA pode determinar que a entidade que pediu o certificado não é quem ele disse eles era, ou a chave privada associou com o certificado pode ser relatada roubado. Os clientes que estão validando uma identidade do servidor de Web baseada em um certificado de servidor assinado podem consultar o CRL para confirmar que o certificado não esteve revogado.

Um CRL contém uma lista de Certificados que foram revogados por CA particular e essa lista é assinada então pelos Certificados revogados CA é identificada pelo número de série. Um cliente pode recuperar este CRL e então confirmar que o certificado de servidor não está alistado no

CRL. A URL para transferir o CRL é incluída geralmente como um campo no certificado. Como uma maneira prática, a maioria de clientes não validam Certificados contra um CRL.

Quando o WSA está decifrando o tráfego HTTPS ou SSL, faz este gerando um certificado de servidor novo e assinando o com seu próprio CA interno **(certificado transferido arquivos pela rede ou gerado sob a seção do proxy HTTPS)**.

Se o WSA não descascou a informação **CRL**, a seguir um cliente que quisesse validar o CRL encontraria que o **certificado** e o **CRL estão assinados por autoridades de certificação diferentes**, e para ignorar o CRL ou para embandeirar um erro. Além disso, sob algumas circunstâncias, o WSA mudará o número de série no certificado gerado para ser diferente do que o número de série no certificado original. Isto significa que, mesmo se um cliente ignorou a diferença em CA entre o CRL e o certificado WSA-gerado, a informação do número de série não seria válida.

A melhor maneira de endereçar a edição é para que o WSA valide o CRL próprio, no interesse do cliente e exclua então a informação CRL do certificado. WSA não é capaz de fazer isto hoje.

Em versões 7.7 e mais recente de AsyncOS:

Começando com versão 7.7 de AsyncOS, o WSA apoia o protocolo em linha do status de certificação (**OCSP**) que é uma alternativa ao CRL.

Quando permitido, OCSP fornece a capacidade para obter o status de revogação de um certificado digital X.509.