Pourquoi WSA élimine-t-il les informations CRL des Certificats générés tout en déchiffrant le trafic HTTPS ?

Contenu

Questions

1. Pourquoi font-elles les informations de la bande CRL des appareils de sécurité Web de Cisco (WSA) des Certificats générés tout en déchiffrant le trafic HTTPS ?
2. Quand générer « a charrié » le certificat de serveur pendant le déchiffrement SSL, le WSA élimine le Liste des révocations de certificat (CRL) du certificat d'origine. Pourquoi est-ce que ceci est fait ?

Environnement

WSA toute version, proxy HTTPS et déchiffrement SSL activé.

Symptômes

Les informations CRL dans le certificat de serveur d'origine ne sont plus présentes dans le certificat généré alors que le trafic de déchiffrage HTTPS sur WSA, et les clients ne peuvent pas confirmer ainsi si le certificat a été retiré.

Le WSA élimine les informations CRL parce qu'il n'est plus valide pour le certificat généré. L'explication implique une compréhension de la façon dont travail de CRLs.

Un Autorité de certification (CA) peut sur option mettre à jour une liste de Certificats qu'elle ne considère plus valides, appelé une liste des révocations de certificat, ou de CRL. Un certificat peut être retiré pour des raisons diverses - le CA peut déterminer que l'entité qui a demandé le certificat n'est pas qui elles a indiqué eux étaient, ou la clé privée a associé avec le certificat peut être signalée dérobé. Les clients qui valident une identité de web server basée sur un certificat de serveur signé peuvent consulter le CRL pour confirmer que le certificat n'a pas été retiré.

Un CRL contient une liste de Certificats qui ont été retirés par un CA particulier et cette liste est alors signée par les Certificats retirés par CA sont identifiées par le numéro de série. Un client peut récupérer ce CRL et puis le confirmer que le certificat de serveur n'est pas répertorié dans le

CRL. L'URL pour télécharger le CRL est habituellement inclus comme un champ dans le certificat. Comme manière pratique, la plupart des clients ne valident pas des Certificats contre un CRL.

Quand le WSA déchiffre le trafic HTTPS ou SSL, il fait ceci en générant un nouveau certificat de serveur et en le signant avec son propre CA interne **(certificat téléchargé ou généré sous la section de proxy HTTPS)**.

Si le WSA n'éliminait pas les informations **CRL**, alors un client qui a voulu valider le CRL constaterait que le **certificat** et les **CRL sont signés par différentes autorités de certification**, et ignorer le CRL ou signaler une erreur. En outre, dans certaines circonstances, le WSA changera le numéro de série dans le certificat généré pour être différent que le numéro de série dans le certificat d'origine. Ceci signifie que, même si un client a ignoré la différence dans le CA entre le CRL et le certificat WSA-généré, les informations de numéro de série ne seraient pas valides.

La meilleure manière d'aborder la question est pour que le WSA valide le CRL lui-même, au nom du client et puis pour exclut les informations CRL du certificat. WSA n'est pas capable de faire ceci aujourd'hui.

Sur des versions 7.7 et ultérieures d'AsyncOS :

Commençant par la version 7.7 d'AsyncOS, le WSA prend en charge l'état en ligne Protocol (**OCSP**) de certification qui est une alternative à CRL.

Une fois activé, OCSP fournit la capacité d'obtenir l'état de révocation d'un certificat numérique X.509.