WSA为什么从生成的证书剥离CRL信息，当解密HTTPS流量时？

目录

问题

1. 为什么从生成的证书的思科Web安全工具(WSA)小条CRL信息，当解密HTTPS流量时？
2. 当生成“在SSL解密时伪装了”服务器证书， WSA从原始证书剥离证书撤销列表(CRL)。 这为什么执行？

环境

WSA任何版本、HTTPS代理和启用的SSL解密。

症状

在原始服务器证书的CRL信息不再是存在生成的证书，当解密在WSA时的HTTPS流量，并且客户端不能因而确认证书是否取消。

因为为生成的证书，不再是有效WSA剥离CRL信息。说明介入了解对Crl如何工作。

Certificate Authority (CA)能或者维护不再认为有效，呼叫证书撤销列表证书，或者CRL的列表。证书可能由于各种各样的原因取消- CA可能确定实体请求的证书不是谁他们说他们是，或者专用密钥关联与证书可能报告窃取。验证根据一签字的服务器证书的Web服务器标识的客户端可能参见CRL确认证书未取消。

CRL包含由特定CA取消，并且该列表由CA.取消的证书然后签字由序列号识别证书的列表。客户端能获取此CRL然后确认服务器证书在CRL没有列出。下载的URL CRL通常包括作为字段在证书。作为实用的方式，多数客户端不验证证书CRL。

当WSA解密HTTPS或SSL流量时，通过生成一新的服务器证书和签署它执行此与其自己的内部CA **(证书上传或生成在HTTPS代理部分下)**。

如果WSA没有剥离CRL信息，则要验证CRL的客户端发现**证书**和**CRL由不同的身份验证权限签字**，和忽略CRL或标记错误。 此外，在一些情况下， WSA跟在原始证书的序列号将更换在生成的证书的序列号不同。这意味着，即使客户端忽略在CA的差异在CRL和WSA生成的证书之间，序列号信息不会有效。

解决问题的最佳方法是为了WSA能验证代表客户端的CRL，然后排除CRL信息从证书。WSA不能够执行此今天。

在AsyncOS版本7.7和以上：

开始与AsyncOS版本7.7， WSA支持是替代方案对CRL的联机证书状态协议(OCSP)。

当启用， OCSP提供能力获取X.509数字证书的废止状态。