WSA가 HTTPS 트래픽을 해독하는 동안 생성된 인증서에서 CRL 정보를 제거하는 이유는 무엇입니까?

목차

[질문](#)
[환경](#)
[증상](#)

질문

1. Cisco WSA(Web Security Appliance)가 HTTPS 트래픽을 해독하는 동안 생성된 인증서에서 CRL 정보를 제거하는 이유는 무엇입니까?
2. SSL 암호 해독 중에 "스푸핑된" 서버 인증서를 생성할 때 WSA는 원본 인증서에서 CRL(인증서 해지 목록)을 제거합니다. 이 작업은 왜 수행됩니까?

환경

WSA 모든 버전, HTTPS 프록시 및 SSL 암호 해독이 활성화되었습니다.

증상

원래 서버 인증서의 CRL 정보는 WSA에서 HTTPS 트래픽을 해독하는 동안 생성된 인증서에 더 이상 존재하지 않으므로, 클라이언트는 인증서가 해지되었는지 여부를 확인할 수 없습니다.

WSA는 생성된 인증서에 대해 더 이상 유효하지 않으므로 CRL 정보를 제거합니다.설명에는 CRL의 작동 방식에 대한 이해가 포함됩니다.

CA(Certificate Authority)는 더 이상 유효하지 않은 것으로 간주되는 인증서 목록, 즉 CRL을 선택적으로 유지 관리할 수 있습니다.인증서는 다양한 이유로 취소될 수 있습니다. CA는 인증서를 요청한 엔티티가 자신이 인증한 엔티티가 아님을 확인할 수 있으며, 인증서와 연결된 개인 키가 도난된 것으로 보고될 수 있습니다.서명된 서버 인증서를 기반으로 웹 서버 ID를 검증하는 클라이언트는 CRL을 참조하여 인증서가 해지되지 않았는지 확인할 수 있습니다.

CRL에는 특정 CA에 의해 폐기된 인증서 목록이 포함되어 있으며, 이 목록은 CA에 의해 서명됩니다.해지된 인증서는 일련 번호로 식별됩니다.클라이언트는 이 CRL을 검색한 다음 서버 인증서가 CRL에 나열되지 않았는지 확인할 수 있습니다.CRL을 다운로드하기 위한 URL은 일반적으로 인증서의 필드로 포함됩니다.실제로 대부분의 클라이언트는 CRL에 대해 인증서를 검증하지 않습니다.

WSA가 HTTPS 또는 SSL 트래픽을 해독하는 경우 새 서버 인증서를 생성하고 자체 내부

CA(**HTTPS 프록시 섹션**에서 **업로드되거나 생성된 인증서)로** 서명하여 이를 수행합니다.

WSA가 **CRL** 정보**를 제거하지 않은 경우** CRL을 검증하려는 클라이언트는 **인증서** 및 **CRL**이 **다른 인증 기관**에 **의해 서명되었음을** 발견하고, CRL을 무시하거나 오류를 플래그 지정합니다. 또한 경우에 따라 WSA는 생성된 인증서의 일련 번호를 원래 인증서의 일련 번호와 다르게 변경합니다.즉, 클라이언트가 CRL과 WSA 생성 인증서 간의 CA의 차이를 무시하더라도 일련 번호 정보가 유효하지 않습니다.

문제를 해결하는 가장 좋은 방법은 WSA가 클라이언트 대신 CRL 자체를 검증한 다음 인증서에서 CRL 정보를 제외하는 것입니다.WSA는 현재 이 작업을 수행할 수 없습니다.

AsyncOS 버전 7.7 이상에서:

AsyncOS 버전 7.7부터 WSA는 CRL의 대안인 **OCSP**(Online Certification Status Protocol)를 지원합니다.

활성화된 경우 OCSP는 X.509 디지털 인증서의 폐기 상태를 가져올 수 있는 기능을 제공합니다.