ASA 및 AnyConnect를 사용할 때 POODLE 및 POODLE에서 사용하는 취약성 방지

목차

소개

이 문서에서는 ASA(Adaptive Security Appliances) 및 SSL(Secure Sockets Layer) 연결을 사용할 때 Padding Oracle On Downgraded Legacy Encryption(POODLE) 취약성을 방지하기 위해 수행해야 하는 작업에 대해 설명합니다.

배경 정보

POODLE 취약성은 TLSv1(Transport Layer Security version 1) 프로토콜의 특정 구현에 영향을 미치며, 인증되지 않은 원격 공격자가 중요한 정보에 액세스하도록 허용할 수 있습니다.

취약성은 CBC(Cipher Block Chaining) 모드를 사용할 때 TLSv1에서 구현된 부적절한 블록 암호 패딩 때문입니다.공격자는 암호화 메시지에 대해 "oracle padding" 사이드 채널 공격을 수행하기 위해 취약성을 악용할 수 있습니다.익스플로잇이 성공하면 공격자가 민감한 정보에 액세스할 수 있습니다.

문제

ASA는 수신 SSL 연결을 두 가지 형식으로 허용합니다.

1. 클라이언트리스 WebVPN
2. AnyConnect 클라이언트

그러나 ASA 또는 AnyConnect 클라이언트에 대한 TLS 구현은 POODLE의 영향을 받지 않습니다.대신 SSLv3을 협상하는 모든 클라이언트(브라우저 또는 AnyConnect)가 이 취약성에 영향을 받도록 SSLv3 구현에 영향을 미칩니다.

> **주의:**그러나 POODLE BITES는 ASA의 TLSv1에 영향을 주지 않습니다.영향을 받는 제품 및 픽스에 대한 자세한 내용은 CVE-2014-8730을 참조하십시오.

솔루션

Cisco는 이 문제를 해결하기 위해 다음과 같은 솔루션을 구현했습니다.

1. 이전에 지원(협상된) SSLv3이 지원되는 모든 AnyConnect 버전은 더 이상 사용되지 않으며 다운로드 가능한 버전(v3.1x 및 v4.0 모두)은 SSLv3을 협상하지 않으므로 문제가 발생할 가능성이 없습니다.

2. ASA의 기본 프로토콜 설정이 SSLv3에서 TLSv1.0으로 변경되었으므로 수신 연결이 TLS를 지원하는 클라이언트에서 오는 한 협상됩니다.

3. ASA는 다음 명령을 사용하여 특정 SSL 프로토콜만 허용하도록 수동으로 구성할 수 있습니다.

   ssl server-version

   솔루션 1에서 설명한 것처럼 현재 지원되는 AnyConnect 클라이언트 중 어떤 것도 SSLv3를 더 이상 협상하지 않으므로 클라이언트는 다음 명령 중 하나로 구성된 ASA에 연결하지 못합니다.
   ```
   ssl server-version sslv3
   ssl server-version sslv3-only
   ```

   그러나 사용되지 않는 v3.0.x 및 v3.1.x AnyConnect 버전(모든 AnyConnect 빌드 버전 PRE 3.1.05182)을 사용하고 SSLv3 협상이 특별히 사용되는 구축의 경우 SSLv3 사용을 제거하거나 클라이언트 업그레이드를 고려하는 유일한 솔루션이 됩니다.

4. POODLE BITES(Cisco 버그 ID CSCus08101)에 대한 실제 픽스는 최신 중간 릴리스 버전에만 통합됩니다.문제를 해결할 수정 사항이 있는 ASA 버전으로 업그레이드할 수 있습니다.Cisco Connection Online(CCO)에서 사용 가능한 첫 번째 버전은 버전 9.3(2.2)입니다.

   이 취약성을 위한 첫 번째 고정 ASA 소프트웨어 릴리스는 다음과 같습니다.
   8.2 기차: 8.2.5.558.4 기차: 8.4.7.269.0 기차: 9.0.4.299.1 기차: 9.1.69.2 기차: 9.2.3.39.3 기차: 9.3.2.2

TLSv1.2

- ASA는 소프트웨어 버전 9.3(2)부터 TLSv1.2를 지원합니다.
- AnyConnect 버전 4.x 클라이언트는 모두 TLSv1.2를 지원합니다.

이는 다음을 의미합니다.

- 클라이언트리스 WebVPN을 사용하는 경우 이 버전의 소프트웨어 이상을 실행하는 모든 ASA에서 TLSv1.2를 협상할 수 있습니다.

- AnyConnect 클라이언트를 사용하는 경우 TLSv1.2를 사용하려면 버전 4.x 클라이언트로 업그레이드해야 합니다.

관련 정보

- CVE-2014-8730
- Cisco 버그 ID CSCug51375
- Cisco 버그 ID CSCur42776
- 기술 지원 및 문서 – Cisco Systems