SSL v3 및 TLS v1 프로토콜 취약점 CBC 모드 취약성

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 CBC(Cipher Block Chaining) 모드 암호화를 비활성화하는 방법에 대해 설명합니다.보안 감사/스캔에서는 ESA에 SSL(Secure Sockets Layer) v3/TLS(Transport Layer Security) v1 Protocol Weak CBC Mode Vulnerability가 있다고 보고할 수 있습니다.

> **주의**:이전 버전의 AsyncOS for Email Security 코드를 실행하는 경우 버전 11.0.3 이상으로 업그레이드하는 것이 좋습니다. 최신 버전 및 정보는 Cisco Email Security 릴리스 정보를 검토하십시오. 암호화 업그레이드 또는 비활성화에 대한 추가 지원이 필요한 경우 지원 케이스를 여십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 AsyncOS for Email Security(모든 수정 버전), Cisco ESA 및 가상 ESA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

- PCI DSS(Payment Card Industry Data Security Standard) 규정 준수를 위해서는 CBC 암호를 비활성화해야 합니다.
- 보안 감사/스캔은 CBC 모드 암호를 사용하는 SSL v3/TLS v1 프로토콜로 잠재적인 취약성을 식별했습니다.

  팁:SSL 버전 3.0(RFC-6101)은 오래되고 안전하지 않은 프로토콜입니다.SSLv3 CVE-2014-3566에 Padding Oracle On Downgraded Legacy Encryption (POODDS) 공격, Cisco 버그 ID CSCur27131로 알려져 있습니다. 암호화를 변경하고 TLS만 사용하고 옵션 3(TLS v1)을 사용하는 동안 SSL v3을 비활성화하는 것이 좋습니다. 제공된 Cisco 버그 ID CSCur27131에서 자세한 내용을 검토합니다.

SSL v3 및 TLS v1 프로토콜은 HTTP 및 LDAP(Lightweight Directory Access Protocol)와 같은 다른 프로토콜에 무결성, 신뢰성 및 프라이버시를 제공하기 위해 사용됩니다. 이러한 서비스는 개인 정보 보호를 위한 암호화, 신뢰성을 위한 x509 인증서, 무결성을 위한 단방향 암호화 기능을 제공합니다.데이터를 암호화하기 위해 SSL 및 TLS는 원본 데이터의 고정 블록만 동일한 크기의 암호화된 블록으로 암호화할 수 있는 암호화 알고리즘인 블록 암호를 사용할 수 있습니다.이러한 암호는 항상 동일한 원본 데이터 블록에 대해 동일한 결과 블록을 가져옵니다.출력의 차이를 달성하기 위해 암호화 출력은 초기화 벡터(IV)라고 하는 동일한 크기의 또 다른 블록과 함께 XORed입니다.CBC는 블록 암호 암호화 출력의 차이를 얻기 위해 초기 블록에 대해 하나의 IV를 사용하고 각 후속 블록에 대해 이전 블록의 결과를 사용합니다.

SSL v3 및 TLS v1 구현에서는 전체 트래픽이 단일 초기 IV 집합과 하나의 CBC 세션을 공유하므로 선택한 CBC 모드 사용량이 낮았습니다.앞서 언급한 대로 나머지 IV는 이전 블록의 암호화 결과입니다.그 다음 정맥주사는 도청자들에게 가능하다.이렇게 하면 공격자가 임의의 트래픽을 일반 텍스트 스트림에 삽입하여(클라이언트에 의해 암호화됨) 삽입된 블록 앞에 있는 일반 텍스트의 추측을 확인할 수 있습니다.공격자의 예측이 정확하면 암호화 출력이 두 블록에 대해 동일합니다.

낮은 엔트로피 데이터의 경우 비교적 적은 수의 시도로 일반 텍스트 블록을 추측할 수 있습니다.예를 들어 1,000개의 가능성이 있는 데이터의 경우 시도 횟수는 500회 가능합니다.

요구 사항

익스플로잇이 작동하려면 몇 가지 요구 사항을 충족해야 합니다.

1. SSL/TLS 연결은 DES 또는 AES와 같은 CBC 모드를 사용하는 블록 암호화 암호 중 하나를 사용해야 합니다. RC4와 같은 스트림 암호를 사용하는 채널은 결함이 발생하지 않습니다 .SSL/TLS 연결의 상당 부분은 RC4를 사용합니다.
2. 취약성은 SSL/TLS 연결에 대한 데이터를 인터셉트하고 해당 연결에 대한 새 데이터를 능동적으로 전송하는 누군가에 의해서만 악용될 수 있습니다.결함이 발생하면 SSL/TLS 연결이 종료됩니다.공격자는 메시지 해독을 위해 충분한 데이터가 수집될 때까지 계속해서 새 연결을 모니터링하고 사용해야 합니다.
3. 연결이 매번 종료되므로 SSL/TLS 클라이언트는 메시지가 해독될 때까지 SSL/TLS 채널을 계속 재설정할 수 있어야 합니다.
4. 애플리케이션은 생성하는 각 SSL/TLS 연결에서 동일한 데이터를 재전송해야 하며, 리스너는 데이터 스트림에서 이를 찾을 수 있어야 합니다.로그인할 고정 메시지 집합이 있는 IMAP/SSL과 같은 프로토콜은 이 요구 사항을 충족합니다.일반 웹 브라우징은 그렇지 않습니다.

위협

CBC 취약성은 TLS v1의 취약성입니다. 이 취약성은 2004년 초부터 존재하며 이후 버전의 TLS v1.1 및 TLS v1.2에서 해결되었습니다.

AsyncOS 9.6 for Email Security 이전에는 ESA에서 TLS v1.0 및 CBC 모드 암호를 사용합니다 .AsyncOS 9.6의 릴리스를 통해 ESA는 TLS v1.2를 도입합니다. 그러나 CBC 모드 암호를 비활성화할 수 있으며 결함이 없는 RC4 암호만 사용할 수 있습니다.

또한 SSLv2가 활성화된 경우 이 취약성에 대해 오탐이 발생할 수 있습니다.SSL v2를 비활성화하는 것이 매우 중요합니다.

솔루션

> **주의**:이전 버전의 AsyncOS for Email Security 코드를 실행하는 경우 버전 11.0.3 이상으로 업그레이드하는 것이 좋습니다. 최신 버전 및 정보는 Cisco Email Security 릴리스 정보를 검토하십시오. 암호화 업그레이드 또는 비활성화에 대한 추가 지원이 필요한 경우 지원 케이스를 여십시오.

RC4 암호만 사용하도록 설정하려면 CBC 모드 암호를 사용하지 않도록 설정합니다.TLS v1 또는 TLS v1/TLS v1.2만 사용하도록 디바이스를 설정합니다.

1. CLI에 로그인합니다.
2. sslconfig 명령을 **입력합니다**.
3. 명령 **GUI**를 **입력합니다**.
4. "TLS v1"에 대해 옵션 번호 3을 선택하거나 AsyncOS 9.6 "TLS v1/TLS v1.2"에 나열된 대로 선택합니다.
5. 암호 입력:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. 다음 명령을 입력합니다.**인바운드**.
7. "TLS v1"에 대해 옵션 번호 3을 선택하거나 AsyncOS 9.6 "TLS v1/TLS v1.2"에 나열된 대로 선택합니다.
8. 암호 입력:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. OUTBOUND 명령을 **입력합니다**.
10. "TLS v1"에 대해 옵션 번호 3을 선택하거나 AsyncOS 9.6 "TLS v1/TLS v1.2"에 나열된 대로 선택합니다.
11. 암호 입력:
    `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
12. 호스트 이름 프롬프트로 돌아갈 때까지 Enter 키를 누릅니다.
13. commit 명령을 **입력합니다**.
14. 변경 사항 커밋을 완료합니다.

이제 ESA는 TLS v1 또는 TLSv1/TLS v1.2만 지원하도록 구성되었으며 RC4 암호는 CBC 필터를 허용하지 않습니다.

다음은 RC4:-SSLv2를 설정할 때 사용되는 암호 목록입니다. 목록에는 CBC 모드 암호가 없습니다.

```
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
```

```
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

이 익스플로잇은 익스플로잇의 복잡성과 취약점 때문에 매우 우려하지 않지만, 이러한 단계의 성능은 익스플로잇을 방지하는 것은 물론 엄격한 보안 검사를 통과하기 위한 훌륭한 보호책입니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems