ASA BEAST 취약성 솔루션

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 소프트웨어 내에서 권한이 없는 사용자가 보호된 콘텐츠에 액세스할 수 있는 취약성에 대해 설명합니다. 이 문제에 대한 해결 방법도 설명합니다.

문제

공격자가 SSL/TLS(BEAST)에 대한 브라우저 익스플로잇 취약성을 활용하여 알려진 일반 텍스트 공격으로 CBC(Cipher Block Chaining) 암호화 모드에서 IV(Initialization Vector) 체이닝을 통해 보호된 콘텐츠를 효과적으로 읽습니다.

이 공격은 널리 사용되는 TLSv1(Transport Layer Security Version 1) 프로토콜에서 취약성을 악용하는 툴을 사용합니다. 이 문제는 프로토콜 자체에 있는 것이 아니라 사용하는 암호 그룹에 있습니다. TLSv1 및 SSLv3(Secure Sockets Layer Version 3)은 CBC 암호를 선호하며, 여기서 Padding Oracle 공격이 발생합니다.

사용자 영향

Trustworthy Internet Movement에서 생성한 SSL Pulse SSL 구현 설문조사에서 알 수 있듯이 SSL 서버의 75% 이상이 이 취약성에 취약합니다. 그러나 BEAST 툴과 관련된 물류 체계는 매우 복잡합니다. BEAST를 사용하여 트래픽을 엿보려면 공격자는 패킷을 매우 빠르게 읽고 삽입할 수 있는 능력을 가져야 합니다. 이는 잠재적으로 BEAST 공격의 유효 대상을 제한합니다. 예를 들어, BEAST 공격자는 WIFI 핫스팟 또는 제한된 수의 네트워크 게이트웨이를 통해 모든 인터넷 트래픽이 병목 현상이 발생하는 곳에서 무작위 트래픽을 효과적으로 잡을 수 있습니다.

솔루션

BEAST는 프로토콜에 의해 사용되는 암호의 취약점을 악용하는 것입니다. CBC 암호에는 영향을 주므로 이 문제를 해결할 수 있는 원래 방법은 RC4 암호로 전환하는 것이었습니다. 그러나 2013년에 발표된 RC4 문서의 Key Scheduling Algorithm의 약점은 RC4도 약점이 있어 부적합하다는 것을

보여줍니다.

이 문제를 해결하기 위해 Cisco는 ASA에 다음 두 가지 수정 사항을 구현했습니다.

- Cisco 버그 ID CSCts83720: *TLS 1.1/1.2으로 업그레이드*

  TLS 1.1/1.2을 업그레이드하고 사용합니다. 이 솔루션의 제한 사항은 ASA 5500-X ASA 플랫폼에만 적용된다는 것입니다. 레거시 ASA 플랫폼(ASA 5505 및 ASA 5500 시리즈)의 암호화 하드웨어는 TLSv1.2를 지원하지 않습니다. 따라서 이러한 플랫폼에 대한 수정 작업은 실행할 수 없습니다.

  프로토콜 제한 때문에 SSLv3 또는 TLSv1.0에 대한 솔루션은 없습니다. 그러나 대부분의 최신 브라우저는 다양한 차단 방법을 구현했습니다.

- Cisco 버그 ID CSCuc85781: *WebVPN 쿠키 임의 설정*

  TLSv1.2를 지원하지 않는 ASA 소프트웨어 버전의 경우, Cisco는 위험을 줄이기 위해 이 수정으로 쿠키를 임의로 만들었습니다. 이는 BEAST 공격을 완전히 차단하지는 않지만, 이를 완화하는 데 도움이 됩니다.

  팁: BEAST 취약성으로부터 완전히 보호하는 유일한 방법은 TLSv1.2를 사용하는 것입니다. 이는 암호와 유사합니다. Cisco는 계속해서 새로운 코드에 더 새롭고 강력한 암호를 추가하며, 오래된 암호에는 알려진 문제(예: RC4)가 있을 수 있습니다. 따라서 최신 프로토콜과 암호로 이동하는 것이 좋습니다.