ASA BEAST-Schwachstellen-Lösungen

Inhalt

Einführung

In diesem Dokument wird eine Schwachstelle in der Cisco Adaptive Security Appliance (ASA)-Software beschrieben, die unbefugten Benutzern den Zugriff auf geschützte Inhalte ermöglicht. Problemumgehungen für dieses Problem werden ebenfalls beschrieben.

Problem

Die Browser Exploit Against SSL/TLS (BEAST)-Schwachstelle wird von einem Angreifer genutzt, um geschützte Inhalte über Initialization Vector (IV) Chaining im Cipher Block Chaining (CBC)-Verschlüsselungsmodus mit einem bekannten Klartextangriff effektiv zu lesen.

Der Angriff nutzt ein Tool, das eine Schwachstelle im weit verbreiteten TLSv1-Protokoll (Transport Layer Security Version 1) ausnutzt. Das Problem beruht nicht auf dem Protokoll selbst, sondern auf den Verschlüsselungssuiten, die es verwendet. TLSv1 und SSLv3 (Secure Sockets Layer Version 3) bevorzugen CBC-Verschlüsselungen, bei denen der Padding-Oracle-Angriff erfolgt.

Auswirkungen auf Benutzer

Wie aus der SSL Pulse SSL Implementation Survey hervorgeht, die von der Trustable Internet Movement erstellt wurde, sind über 75 % der SSL-Server anfällig für diese Schwachstelle. Allerdings ist die Logistik im Zusammenhang mit dem BEAST-Tool ziemlich kompliziert. Um BEAST zum Abhören von Datenverkehr verwenden zu können, muss ein Angreifer in der Lage sein, Pakete sehr schnell zu lesen und einzuschleusen. Dies schränkt möglicherweise die effektiven Ziele für einen BEAST-Angriff ein. Ein BEAST-Angreifer kann beispielsweise Zufallsdatenverkehr an einem WIFI-Hotspot erfassen oder den gesamten Internetdatenverkehr über eine begrenzte Anzahl von Netzwerk-Gateways blockieren.

Lösung

BEAST ist ein Exploit der Schwäche in der Chiffre, die vom Protokoll verwendet wird. Da es sich

auf die CBC-Chiffre auswirkt, bestand die ursprüngliche Problemumgehung für dieses Problem darin, stattdessen auf die RC4-Chiffre zu wechseln. Die Schwächen im Key Scheduling Algorithm des RC4-Artikels, der 2013 veröffentlicht wurde, zeigen jedoch, dass selbst RC4 eine Schwäche hatte, die es ungeeignet machte.

Um dieses Problem zu umgehen, hat Cisco die folgenden beiden Fixes für die ASA implementiert:

- Cisco Bug ID CSCts83720: *Upgrade auf TLS 1.1/1.2*

  Aktualisieren und verwenden Sie TLS 1.1/1.2. Die Einschränkung bei dieser Lösung besteht darin, dass sie nur für ASA 5500-X ASA-Plattformen gilt. Die Verschlüsselungshardware auf älteren ASA-Plattformen (ASA 5505 und ASA 5500-Serie) unterstützt TLSv1.2 nicht. Infolgedessen ist eine Behebung dieser Plattformen nicht möglich.

  Aufgrund von Protokollbeschränkungen gibt es keine Lösung für SSLv3 oder TLSv1.0. Die meisten modernen Browser haben jedoch verschiedene Methoden zur Eindämmung von Bedrohungen implementiert.

- Cisco Bug-ID CSCuc85781: *WebVPN-Cookie-Randomisierung*

  Für die ASA-Softwareversionen, die TLSv1.2 nicht unterstützen, hat Cisco die Cookies zufällig mit diesem Fix erstellt, um das Risiko zu verringern. Dies verhindert zwar nicht vollständig BEAST-Angriffe, hilft aber, diese abzuwehren.

  Tipp: Die einzige Möglichkeit, um vollständig vor der BEAST-Schwachstelle geschützt zu sein, ist die Verwendung von TLSv1.2. Das ist vergleichbar mit Chiffren. Cisco fügt auch weiterhin neuere, stärkere Chiffren in neueren Code hinzu, und ältere Chiffren können bekannte Probleme aufweisen (z. B. RC4). Cisco empfiehlt daher, zu den neueren Protokollen und Chiffren zu wechseln.