Solutions de vulnérabilité ASA BEAST

Contenu

Introduction

Ce document décrit une vulnérabilité au sein du logiciel Cisco Adaptive Security Appliance (ASA) qui permet aux utilisateurs non autorisés d'accéder au contenu protégé. Les solutions à ce problème sont également décrites.

Problème

La vulnérabilité du navigateur Exploit Against SSL/TLS (BEAST) est exploitée par un pirate afin de lire efficacement le contenu protégé via Initialization Vector (IV) chacking en mode de chiffrement Cipher Block Chaining (CBC) avec une attaque en texte clair connue.

L'attaque utilise un outil qui exploite une vulnérabilité dans le protocole TLSv1 (Transport Layer Security Version 1), très utilisé. Le problème ne trouve pas son origine dans le protocole lui-même, mais plutôt dans les suites de chiffrement qu'il utilise. Le protocole TLSv1 et le protocole SSLv3 (Secure Sockets Layer Version 3) favorisent les algorithmes de chiffrement CBC, où l'attaque Oracle Padding se produit.

Impact de l'utilisateur

Comme l'indique l'enquête de mise en oeuvre SSL Pulse SSL, créée par le Trustworthy Internet Movement, plus de 75 % des serveurs SSL sont sensibles à cette vulnérabilité. Cependant, la logistique associée à l'outil BEAST est assez compliquée. Afin d'utiliser BEAST pour intercepter le trafic, un pirate doit avoir la capacité de lire et d'injecter des paquets très rapidement. Cela pourrait limiter les cibles efficaces d'une attaque BEAST. Par exemple, un pirate BEAST peut effectivement saisir du trafic aléatoire sur un point d'accès WIFI ou lorsque tout le trafic Internet est bloqué par un nombre limité de passerelles réseau.

Solution

BEAST est une exploitation de la faiblesse du chiffre utilisé par le protocole. Étant donné qu'il

affecte le chiffrement CBC, la solution de contournement originale pour ce numéro était de passer au chiffrement RC4 à la place. Cependant, les faiblesses de l'algorithme de programmation clé de l'article RC4 publié en 2013 révèlent que même RC4 avait une faiblesse qui le rendait inapproprié.

Afin de résoudre ce problème, Cisco a mis en oeuvre les deux correctifs suivants pour l'ASA :

- ID de bogue Cisco CSCts83720 : *Mise à niveau vers TLS 1.1/1.2*

  Mettre à niveau et utiliser TLS 1.1/1.2. La limite avec cette solution est qu'elle s'applique uniquement aux plates-formes ASA 5500-X. Le matériel de chiffrement sur les plates-formes ASA existantes (ASA 5505 et ASA 5500) ne prend pas en charge TLSv1.2. Par conséquent, une solution pour ces plates-formes n'est pas possible.

  En raison de limitations de protocole, il n'existe aucune solution pour SSLv3 ou TLSv1.0 ; cependant, la plupart des navigateurs modernes ont mis en oeuvre différentes méthodes d'atténuation.

- ID de bogue Cisco CSCuc85781 : *Récupération aléatoire des cookies WebVPN*

  Pour les versions du logiciel ASA qui ne prennent pas en charge TLSv1.2, Cisco a rendu les cookies aléatoires avec cette correction afin de réduire les risques. Cela n'empêche pas complètement les attaques BEAST, mais contribue à les atténuer.

  Conseil : la seule façon d'être complètement protégé de la vulnérabilité BEAST est d'utiliser TLSv1.2. C'est similaire aux chiffrements. Cisco continue d'ajouter des chiffrements plus récents et plus puissants dans le code le plus récent, et les chiffrements plus anciens peuvent avoir des problèmes connus (par exemple RC4). Par conséquent, Cisco vous recommande de passer aux protocoles et aux algorithmes de chiffrement les plus récents.