Soluciones de vulnerabilidad de ASA BEAST

Contenido

Introducción

Este documento describe una vulnerabilidad dentro del software Cisco Adaptive Security Appliance (ASA) que permite a los usuarios no autorizados acceder al contenido protegido. También se describen las soluciones temporales para este problema.

Problema

Un atacante aprovecha la vulnerabilidad de Browser Exploit Against SSL/TLS (BEAST) para leer de forma efectiva el contenido protegido a través del encadenamiento del vector de inicialización (IV) en el modo de cifrado Cipher Block Chaining (CBC) con un ataque de texto sin formato conocido.

El ataque utiliza una herramienta que explota una vulnerabilidad en el protocolo de seguridad de la capa de transporte versión 1 (TLSv1), ampliamente utilizado. El problema no está enraizado en el protocolo en sí, sino en los conjuntos de aplicaciones cifrados que utiliza. TLSv1 y Secure Sockets Layer versión 3 (SSLv3) favorecen a los cifradores de CBC, donde se produce el ataque de Oracle de relleno.

Impacto del usuario

Como lo indica la encuesta de implementación SSL Pulse, creada por el Movimiento de Internet de Confianza, más del 75% de los servidores SSL son susceptibles a esta vulnerabilidad. Sin embargo, la logística de la herramienta BEAST es bastante complicada. Para utilizar BEAST para interceptar el tráfico, un atacante debe tener la capacidad de leer e inyectar paquetes muy rápidamente. Esto potencialmente limita los objetivos efectivos para un ataque BEAST. Por ejemplo, un atacante BEAST puede captar de forma eficaz el tráfico aleatorio en un punto de conexión WIFI o en el que todo el tráfico de Internet se cuelga a través de un número limitado de gateways de red.

Solución

BEAST es un aprovechamiento de la debilidad en el cifrado que utiliza el protocolo. Como afecta al cifrado de CBC, la solución original para este problema fue cambiar al cifrado RC4 en su lugar. Sin embargo, las Deficiencias del artículo Key Schedule Algorithm de RC4 publicado en 2013 revelan que incluso RC4 tenía una debilidad que la hacía inadecuada.

Para solucionar este problema, Cisco ha implementado estas dos correcciones para ASA:

- Id. de bug Cisco CSCts83720: *Actualización a TLS 1.1/1.2*

  Actualice y utilice TLS 1.1/1.2. La limitación de esta solución es que solo se aplica a las plataformas ASA 5500-X. El hardware de cifrado de las plataformas ASA antiguas (ASA serie 5505 y ASA serie 5500) no admite TLSv1.2. Como resultado, una solución para estas plataformas no es factible.

  Debido a las limitaciones de protocolo, no hay solución para SSLv3 o TLSv1.0; sin embargo, la mayoría de los navegadores modernos han implementado diferentes formas de mitigación.

- Id. de bug Cisco CSCuc85781: *Randomization de cookies de WebVPN*

  Para las versiones de software ASA que no admiten TLSv1.2, Cisco realizó las cookies aleatoriamente con esta corrección para reducir el riesgo. Esto no previene completamente los ataques BEST, pero ayuda a mitigarlos.

  Consejo: La única forma de protegerse completamente de la vulnerabilidad BEAST es utilizar TLSv1.2. Esto es similar a cifras. Cisco continúa añadiendo cifras más recientes y fiables en código más reciente, y las cifras más antiguas podrían tener problemas conocidos (como RC4). Por lo tanto, Cisco recomienda pasar a los protocolos y cifras más recientes.