Evite la vulnerabilidad del CANICHE y de las MORDEDURAS del CANICHE cuando usted utiliza el ASA y AnyConnect

ID del Documento: 118780

Actualizado: Mayo 06, 2015

Contribuido por Atri Basu, ingeniero de Cisco TAC.

Productos Relacionados

- Cisco AnyConnect VPN Client
- Software adaptante del dispositivo de seguridad de Cisco (ASA)
- Secure Socket Layer (SSL)
- Cliente de movilidad Cisco AnyConnect Secure
- Firewall de la última generación de las 5500-X Series de Cisco ASA

Contenido

Introducción

Este documento describe lo que usted debe hacer para evitar el Oracle del relleno en la vulnerabilidad del cifrado de la herencia Downgraded (CANICHE) cuando usted utiliza los dispositivos de seguridad adaptantes (ASA) y AnyConnect para la Conectividad de Secure Sockets Layer (SSL).

Antecedentes

Aplicaciones de las influencias de la vulnerabilidad del CANICHE las ciertas del protocolo de la versión 1 de Transport Layer Security (TLSv1) y podrían permitir que un unauthenticated, atacante remoto acceda la información vulnerable.

La vulnerabilidad es debido al relleno incorrecto del cifrado en bloque implementado en TLSv1 cuando usted utiliza el modo del Cipher Block Chaining (CBC). Un atacante podía explotar la vulnerabilidad para realizar “un ataque del lado-canal del relleno del oráculo” en el mensaje criptográfico. Un exploit acertado podía permitir que el atacante acceda la información vulnerable.

Problema

El ASA permite las conexiones SSL entrantes en dos formas:

1. WebVPN del clientless
2. Cliente de AnyConnect

Sin embargo, no se afecta ningunas de las implementaciones de TLS en el ASA o el cliente de AnyConnect por el CANICHE. En lugar, la implementación SSLv3 es afectada de modo que cualquier cliente (navegador o AnyConnect) que negocia SSLv3 sea susceptible a esta vulnerabilidad.

> Precaución: Las MORDEDURAS del CANICHE sin embargo afectan al TLSv1 en el ASA. Para más información sobre los Productos y los arreglos afectados, refiera a CVE-2014-8730.

Solución

Cisco ha implementado estas soluciones a este problema:

1. Todas las versiones AnyConnect se han desaprobado que soportaron previamente SSLv3 (negociado) y las versiones disponibles para la descarga (v3.1x y v4.0) no negociarán SSLv3 así que de las ellas no son susceptibles al problema.

2. La configuración del protocolo del valor por defecto ASA se ha cambiado de SSLv3 a TLSv1.0 de modo que mientras la conexión entrante sea de un cliente que soporte TLS, eso sea qué será negociada.

3. El ASA se puede configurar manualmente para validar solamente los Protocolos SSL específicos con este comando:

   `ssl server-version`
   Como se menciona en la solución 1, ningunos de los clientes actualmente soportados de AnyConnect negocian SSLv3 más, así que el cliente no podrá conectar con ningún ASA configurado con cualquiera de estos comandos:`ssl server-version sslv3`
   `ssl server-version sslv3-only`

Sin embargo, para las implementaciones que utilizan las versiones v3.0.x y v3.1.x AnyConnect se han desaprobado que (que son todas las versiones PRE 3.1.05182 de la estructura de AnyConnect), y en qué negociación SSLv3 se utiliza específicamente, la única solución es eliminar el uso de SSLv3 o considerar una actualización del cliente.

4. El arreglo real para las MORDEDURAS del CANICHE (Id. de bug Cisco CSCus08101) será integrado en las últimas versiones de versión interina solamente. Usted puede actualizar a una Versión de ASA que tenga el arreglo para solucionar el problema. La primera versión disponible en el Cisco Connection Online (CCO) es versión 9.3(2.2).

   Las primeras versiones de software fijas ASA para esta vulnerabilidad son como sigue: **8.2 Tren: 8.2.5.558.4 Tren: 8.4.7.269.0 Tren: 9.0.4.299.1 Tren: 9.1.69.2 Tren: 9.2.3.39.3 Tren: 9.3.2.2**

TLSv1.2

- El ASA soporta TLSv1.2 a partir de la versión de software 9.3(2).
- Los clientes todos de la versión 4.x de AnyConnect soportan TLSv1.2.

Esto significa:

- Si usted utiliza el WebVPN del clientless, después cualquier ASA que funcione con esta versión de software o más arriba puede negociar TLSv1.2.

- Si usted utiliza al cliente de AnyConnect, para utilizar TLSv1.2, usted necesitará actualizar a los clientes de la versión 4.x.

Información Relacionada

- CVE-2014-8730
- Id. de bug Cisco CSCug51375
- Id. de bug Cisco CSCur42776
- Soporte Técnico y Documentación - Cisco Systems

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Actualizado: Mayo 06, 2015
ID del Documento: 118780