Evite la vulnerabilidad de POODLE y POODLE BITES al utilizar ASA y AnyConnect

Contenido

Introducción

Este documento describe lo que debe hacer para evitar la vulnerabilidad de Oracle On Downgraded Legacy Encryption (POODLE) cuando utiliza Adaptive Security Appliances (ASA) y AnyConnect para la conectividad de Secure Sockets Layer (SSL).

Antecedentes

La vulnerabilidad POODLE afecta a determinadas implementaciones del protocolo Transport Layer Security versión 1 (TLSv1) y podría permitir que un atacante remoto no autenticado acceda a información confidencial.

La vulnerabilidad se debe a un relleno incorrecto del cifrado de bloques implementado en TLSv1 cuando se utiliza el modo Cipher Block Chaining (CBC). Un atacante podría explotar la vulnerabilidad para realizar un ataque de canal lateral "oracle padding" en el mensaje criptográfico. Una explotación exitosa podría permitir al atacante acceder a información confidencial.

Problema

ASA permite conexiones SSL entrantes de dos formas:

1. WebVPN sin cliente
2. Cliente AnyConnect

Sin embargo, POODLE no afecta a ninguna de las implementaciones de TLS en el ASA o el cliente AnyConnect. En su lugar, la implementación de SSLv3 se ve afectada de modo que cualquier cliente (navegador o AnyConnect) que negocie SSLv3 sea susceptible a esta vulnerabilidad.

> **Precaución:** POODLE BITES no obstante afecta a TLSv1 en el ASA. Para obtener más información sobre los productos y soluciones afectados, consulte CVE-2014-8730.

Solución

Cisco ha implementado estas soluciones para este problema:

1. Todas las versiones de AnyConnect que anteriormente admitían (negociadas) SSLv3 han quedado obsoletas y las versiones disponibles para descargar (v3.1x y v4.0) no negociarán SSLv3, por lo que no son susceptibles al problema.

2. La configuración del protocolo predeterminado de ASA se ha cambiado de SSLv3 a TLSv1.0 de modo que mientras la conexión entrante provenga de un cliente que soporte TLS, eso es lo que se negociará.

3. El ASA se puede configurar manualmente para aceptar sólo protocolos SSL específicos con este comando:

   `ssl server-version`

   Como se mencionó en la solución 1, ninguno de los clientes de AnyConnect admitidos actualmente negocia SSLv3, por lo que el cliente no podrá conectarse a 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 de AnyConnect v3.0.x y v3.1.x que han sido obsoletas (que son todas las versiones de compilación de AnyConnect PRE 3.1.05182) y en las que se utiliza específicamente la negociación SSLv3, la única solución es eliminar el uso de SSLv3 o considerar una actualización del cliente.

4. La solución real para POODLE BITES (Cisco bug ID CSCus08101) se integrará solamente en las últimas versiones de la versión provisional. Puede actualizar a una versión de ASA que tenga la solución para resolver el problema. La primera versión disponible en Cisco Connection Online (CCO) es la versión 9.3(2.2).

   Las primeras versiones de software ASA fijas para esta vulnerabilidad son las siguientes: **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 admite TLSv1.2 a partir de la versión de software 9.3(2).
- Todos los clientes de AnyConnect versión 4.x admiten TLSv1.2.

Esto significa:

- Si utiliza WebVPN sin cliente, cualquier ASA que ejecute esta versión de software o superior puede negociar TLSv1.2.

- Si utiliza el cliente AnyConnect, para utilizar TLSv1.2, deberá 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