Evite a vulnerabilidade POODLE e POODLE BITES ao usar o ASA e o AnyConnect

Contents

Introduction

Este documento descreve o que você deve fazer para evitar a vulnerabilidade Padding Oracle On Downgrade Legacy Encryption (POODLE) quando você usa Adaptive Security Appliances (ASAs) e AnyConnect para conectividade Secure Sockets Layer (SSL).

Informações de Apoio

A vulnerabilidade POODLE afeta certas implementações do protocolo TLSv1 (Transport Layer Security versão 1) e pode permitir que um invasor remoto não autenticado acesse informações confidenciais.

A vulnerabilidade se deve ao preenchimento incorreto de cifras de blocos implementado no TLSv1 quando você usa o modo CBC (Cipher Block Chaining). Um invasor pode explorar a vulnerabilidade para executar um ataque de canal lado "oracle padding" na mensagem criptográfica. Uma exploração bem-sucedida pode permitir que o invasor acesse informações confidenciais.

Problema

O ASA permite conexões SSL de entrada de duas formas:

1. WebVPN sem cliente
2. Cliente AnyConnect

No entanto, nenhuma das implementações TLS no ASA ou no cliente AnyConnect é afetada pelo POODLE. Em vez disso, a implementação de SSLv3 é afetada para que todos os clientes (navegador ou AnyConnect) que negociam SSLv3 sejam susceptíveis a essa vulnerabilidade.

> **Caution**: O POODLE BITES, no entanto, afeta o TLSv1 no ASA. Para obter mais informações sobre produtos e correções afetados, consulte CVE-2014-8730.

Solução

A Cisco implementou estas soluções para este problema:

1. Todas as versões do AnyConnect que anteriormente suportavam (negociavam) SSLv3 foram preteridas e as versões disponíveis para download (v3.1x e v4.0) não negociarão o SSLv3, portanto, não são susceptíveis ao problema.

2. A configuração do protocolo padrão do ASA foi alterada de SSLv3 para TLSv1.0 de modo que, desde que a conexão de entrada seja de um cliente que suporte TLS, isso será negociado.

3. O ASA pode ser configurado manualmente para aceitar somente protocolos SSL específicos com este comando:

   `ssl server-version`

   Como mencionado na solução 1, nenhum dos clientes AnyConnect atualmente suportados negocia mais SSLv3, portanto, o cliente não conseguirá se conectar a qualquer ASA configurado com qualquer um destes comandos:

   ```
   ssl server-version sslv3
   ssl server-version sslv3-only
   ```

   No entanto, para implantações que usam as versões v3.0.x e v3.1.x do AnyConnect que foram obsoletas (todas as versões de build do AnyConnect PRE 3.1.05182) e nas quais a negociação SSLv3 é usada especificamente, a única solução é eliminar o uso de SSLv3 ou considerar uma atualização de cliente.

4. A correção real para POODLE BITES (ID de bug da Cisco CSCus08101) será integrada somente nas versões de versão intermediária mais recentes. Você pode atualizar para uma versão ASA que tenha a correção para resolver o problema. A primeira versão disponível no Cisco Connection Online (CCO) é a versão 9.3(2.2).

   As primeiras versões fixas do software ASA para essa vulnerabilidade são as seguintes: **8.2 Comboio: 8.2.5.558.4 Comboio: 8.4.7.269.0 Comboio: 9.0.4.299.1 Comboio: 9.1.69.2.3.3 Comboio: 9.2.39.3.2.2 Comboio**

TLSv1.2

- O ASA oferece suporte ao TLSv1.2 a partir da versão de software 9.3(2).
- Todos os clientes AnyConnect versão 4.x suportam TLSv1.2.

Isso significa:

- Se você usar o Clientless WebVPN, qualquer ASA que executa esta versão de software ou superior poderá negociar o TLSv1.2.

- Se você usar o cliente AnyConnect, para usar TLSv1.2, precisará atualizar para clientes da versão 4.x.

Informações Relacionadas

- CVE-2014-8730
- ID de bug Cisco CSCug51375
- ID de bug Cisco CSCur42776
- Suporte Técnico e Documentação - Cisco Systems