Soluções de vulnerabilidade ASA BEAST

Contents

Introduction

Este documento descreve uma vulnerabilidade no software Cisco Adaptive Security Appliance (ASA) que permite que usuários não autorizados acessem conteúdo protegido. As alternativas para esse problema também são descritas.

Problema

A vulnerabilidade do Browser Exploit Against SSL/TLS (BEAST) é aproveitada por um invasor para ler conteúdo protegido com eficiência através do encadeamento do Initialization Vetor (IV) no modo de criptografia Cipher Block Chaining (CBC) com um conhecido ataque de texto não criptografado.

O ataque usa uma ferramenta que explora uma vulnerabilidade no protocolo TLSv1 (Transport Layer Security Version 1), amplamente usado. A questão não está enraizada no protocolo em si, mas sim nos pacotes de cifras que ele usa. O TLSv1 e o Secure Sockets Layer Version 3 (SSLv3) favorecem cifras de CBC, onde o ataque Oracle Padding ocorre.

Impacto no usuário

Conforme indicado pela pesquisa de implementação SSL Pulse SSL, criada pelo Trustworthy Internet Movement, mais de 75% dos servidores SSL são susceptíveis a essa vulnerabilidade. No entanto, a logística envolvida com a ferramenta BEAST é bastante complicada. Para usar o BEAST para escutar o tráfego, um invasor deve ter a capacidade de ler e injetar pacotes muito rapidamente. Isso potencialmente limita os alvos efetivos de um ataque BEAST. Por exemplo, um invasor BEAST pode efetivamente capturar tráfego aleatório em um ponto de conexão WIFI ou onde todo o tráfego da Internet é bloqueado por meio de um número limitado de gateways de rede.

Solução

O BEAST é uma exploração da fraqueza na cifra usada pelo protocolo. Já que afeta a cifra CBC, a solução original para esse problema era mudar para a cifra RC4. No entanto, os pontos fracos do artigo do RC4, publicado em 2013, revelam que mesmo o RC4 tinha uma fraqueza que o tornava inadequado.

Para contornar esse problema, a Cisco implementou estas duas correções para o ASA:

- ID de bug da Cisco CSCts83720: *Atualizar para TLS 1.1/1.2*

  Atualize e use TLS 1.1/1.2. A limitação com essa solução é que ela se aplica somente às plataformas ASA 5500-X ASA. O hardware de criptografia em plataformas ASA legadas (ASA 5505 e ASA 5500 Series) não oferece suporte ao TLSv1.2. Como resultado, uma correção para essas plataformas não é viável.

  Devido a limitações de protocolo, não há solução para SSLv3 ou TLSv1.0; no entanto, a maioria dos navegadores modernos implementou diferentes formas de mitigação.

- ID de bug da Cisco CSCuc85781: *Randomização de cookies WebVPN*

  Para as versões do software ASA que não suportam TLSv1.2, a Cisco tornou os cookies aleatórios com essa correção para reduzir o risco. Isso não evita completamente os ataques BEAST, mas ajuda a atenuá-los.

  Dica: a única maneira de se proteger completamente da vulnerabilidade do BEAST é usar o TLSv1.2. Isso é parecido com cifras. A Cisco continua a adicionar cifras mais novas e mais fortes em código mais novo, e cifras mais antigas podem ter problemas conhecidos (como RC4). Assim, a Cisco recomenda que você mude para os protocolos e cifras mais novos.