Soluções da vulnerabilidade do ANIMAL ASA

Índice

[Introdução](#)
[Problema](#)
[Impacto do usuário](#)
[Solução](#)

Introdução

Este documento descreve uma vulnerabilidade dentro do sowftware adaptável da ferramenta de segurança de Cisco (ASA) que permite que os usuários não autorizados alcancem o índice protegido. As ações alternativas para esta edição são descritas igualmente.

Problema

A façanha do navegador contra a vulnerabilidade SSL/TLS (ANIMAL) leveraged por um atacante a fim ler eficazmente o índice protegido através do vetor de inicialização (iv) que acorrenta no modo de criptografia do Cipher Block Chaining (CBC) com um ataque conhecido do texto simples.

O ataque usa uma ferramenta que explore uma vulnerabilidade no protocolo amplamente utilizado da versão 1 do Transport Layer Security (TLSv1). A edição não é enraizada no protocolo próprio, mas um pouco nas séries da cifra que usa. A versão 3 TLSv1 e de secure sockets layer (SSLv3) favorece as cifras CBC, onde o ataque do Oracle do estofamento ocorre.

Impacto do usuário

Como indicado pela avaliação da aplicação do pulso SSL SSL, criada pelo movimento de confiança do Internet, sobre 75% dos servidores SSL seja susceptível a esta vulnerabilidade. Contudo, as logísticas envolvidas com a ferramenta do ANIMAL são razoavelmente complicadas. A fim usar o ANIMAL para bisbilhotar no tráfego, um atacante deve ter a capacidade para ler muito rapidamente e injetar pacotes. Isto limita potencialmente os alvos eficazes para um ataque do ANIMAL. Por exemplo, um atacante do ANIMAL pode eficazmente agarrar o tráfego aleatório em um ponto ativo de WIFI ou onde todo o tráfego do Internet bottlenecked através de um número limitado de gateways da rede.

Solução

O ANIMAL é uma façanha da fraqueza na cifra que é usada pelo protocolo. Desde que afeta a

cifra CBC, a ação alternativa original para esta edição era comutar pelo contrário à cifra RC4. Contudo, as fraquezas no algoritmo de escalonamento chave do artigo RC4 que foi publicado em 2013 revelam que mesmo o RC4 teve uma fraqueza que o faça inoportuno.

A ação alternativa esta edição, Cisco executou estes dois reparos para o ASA:

- Identificação de bug Cisco CSCts83720: *Promova a TLS 1.1/1.2*

  Promova e use TLS 1.1/1.2. A limitação com esta solução é que se aplica somente às Plataformas ASA 5500-X ASA. O hardware de criptografia em Plataformas do legado ASA (ASA 5505 e o 5500 Series ASA) não apoia TLSv1.2. Em consequência, um reparo para estas Plataformas não é praticável.

  Devido às limitações de protocolo, não há nenhuma solução para SSLv3 ou TLSv1.0; contudo, a maioria de navegadores modernos executaram maneiras diferentes de mitigação.

- Identificação de bug Cisco CSCuc85781: *Randomization do Cookie WebVPN*

  Para as versões de software ASA que não apoiam TLSv1.2, Cisco fez os Cookie aleatórios com este reparo a fim reduzir o risco. Isto não impede completamente ataques do ANIMAL, mas ajuda a abrandá-los.

  Dica: A única maneira de ser protegido completamente da vulnerabilidade do ANIMAL é usar TLSv1.2. Isto é similar às cifras. Cisco continua a adicionar umas cifras mais novas, mais fortes em um código mais novo, e umas cifras mais velhas puderam ter problemas conhecidos (tais como o RC4). Assim, Cisco recomenda que você se transporta os protocolos e às cifras mais novos.