

Evite a vulnerabilidade da CANICHE e das MORDIDAS da CANICHE quando você usa o ASA e o AnyConnect



ID do Documento: 118780

Atualizado em: maio 06, 2015

Contribuído por Atri Basu, engenheiro de TAC da Cisco.



[Transferência PDF](#)



[Imprimir](#)

[Feedback](#)

Produtos Relacionados

- [Cisco AnyConnect VPN Client](#)
- [Software adaptável da ferramenta de segurança de Cisco \(ASA\)](#)
- [Secure Socket Layer \(SSL\)](#)
- [Cliente de mobilidade Cisco AnyConnect Secure](#)
- [Firewall da próxima geração do 5500-X Series de Cisco ASA](#)

Índice

[Introdução](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[TLSv1.2](#)

[Informações Relacionadas](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Este documento descreve o que você deve fazer para evitar o Oracle do estofamento na vulnerabilidade da criptografia do legado Downgraded (CANICHE) quando você usa as ferramentas de segurança adaptáveis (ASA) e o AnyConnect para a Conectividade do secure sockets layer (SSL).

Informações de Apoio

Aplicações das influências da vulnerabilidade da CANICHE as determinadas do protocolo da versão 1 do Transport Layer Security (TLSv1) e poderiam permitir que um não-autenticado, atacante remoto alcance a informação sensível.

A vulnerabilidade é devido ao estofamento impróprio da cifra de bloco executado em TLSv1 quando você usa o modo do Cipher Block Chaining (CBC). Um atacante podia explorar a vulnerabilidade a fim executar do “um ataque do lado-canal do estofamento oráculo” na mensagem criptograficamente. Uma façanha bem sucedida podia permitir que o atacante alcance a informação sensível.

Problema

O ASA permite conexões SSL entrantes em dois formulários:

1. Sem clientes WebVPN
2. Cliente de AnyConnect

Contudo, nenhuma das aplicações TLS no ASA ou no cliente de AnyConnect são afetadas pela CANICHE. Em lugar de, a aplicação SSLv3 é afetada de modo que todos os clientes (navegador ou AnyConnect) que negocia SSLv3 são susceptíveis a esta vulnerabilidade.

Cuidado: AS MORDIDAS da CANICHE contudo afetam o TLSv1 no ASA. Para obter mais informações sobre de Produtos e dos reparos afetados, refira [CVE-2014-8730](#).

Solução

Cisco executou estas soluções a este problema:

1. Todas as versões de AnyConnect que apoiaram previamente SSLv3 (negociado) foram suplicadas e as versões disponíveis para a transferência (v3.1x e v4.0) não negociarão SSLv3 assim que delas não são susceptíveis à edição.
2. [A configuração de protocolo do padrão do](#) ASA foi mudada de SSLv3 a TLSv1.0 de modo que enquanto a conexão recebida é de um cliente que apoiasse o TLS, aquele fosse o que será negociado.
3. O ASA pode manualmente ser configurado para aceitar somente protocolos SSL específicos com este comando:

[ssl server-version](#)

Como mencionado na solução 1, nenhuns dos clientes atualmente apoiados de AnyConnect negociam SSLv3 anymore, assim que o cliente não conectará a todo o ASA configurado com o qualquer um destes comandos:
`ssl server-version sslv3`

`ssl server-version sslv3-only`

Contudo, para as disposições que usam as versões v3.0.x e v3.1.x AnyConnect que foram

suplicadas (em que são todas as versões PRE 3.1.05182 da construção de AnyConnect), e no que negociação SSLv3 é usada especificamente, a única solução é eliminar o uso de SSLv3 ou considerar uma elevação do cliente.

4. O reparo real para MORDIDAS da CANICHE (identificação de bug Cisco [CSCus08101](#)) será integrado nas versões de versão temporária as mais atrasadas somente. Você pode promover a uma versão ASA que tenha o reparo para resolver o problema. A primeira versão disponível no Cisco Connection Online (CCO) é versão 9.3(2.2).

Os primeiros software release fixos ASA para esta vulnerabilidade são como segue:

8.2 Trem: 8.2.5.558.4 Trem: 8.4.7.269.0 Trem: 9.0.4.299.1 Trem: 9.1.69.2 Trem:
9.2.3.39.3 Trem: 9.3.2.2

TLsv1.2

- O ASA apoia TLsv1.2 até à data da versão de software 9.3(2).
- Os clientes todos da versão 4.x de AnyConnect apoiam TLsv1.2.

Isto significa:

- Se você usa os sem clientes WebVPN, a seguir todo o ASA que executar esta versão de software ou mais altamente puder negociar TLsv1.2.
- Se você usa o cliente de AnyConnect, a fim usar TLsv1.2, você precisará de promover aos clientes da versão 4.x.

Informações Relacionadas

- [CVE-2014-8730](#)
- [Identificação de bug Cisco CSCug51375](#)
- [Identificação de bug Cisco CSCur42776](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Era este documento útil? [Sim nenhum](#)

Obrigado para seu feedback.

[Abra um caso de suporte](#) (exige um [contrato de serviço Cisco](#).)

Cisco relacionado apoia discussões da comunidade

[Cisco apoia a comunidade](#) é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira [convenções dos dicas técnicas da Cisco](#) para obter informações sobre das convenções usadas neste documento.

Atualizado em: maio 06, 2015

ID do Documento: 118780