Índice

[Introdução](#)
[Por que você recebe um aviso sobre a criptografia SSLv3 em CRE?](#)

Introdução

Este documento descreve um aviso sobre a Segurança de sua conexão que você pôde encontrar quando você abre um envelope cifrado registrado Cisco do serviço do envelope (CRE) ou visita o Web site CRE se você usa a versão 3 do secure sockets layer (SSLv3). Embora você possa ainda alcançar o envelope cifrado e o Web site CRE, é importante que você está ciente dos riscos de segurança potencial envolvidos com o uso de SSLv3 em seu navegador.

Por que você recebe um aviso sobre a criptografia SSLv3 em CRE?

Você recebe o aviso porque os server CRE detectaram que seu navegador da Web negociou uma conexão SSLv3. O protocolo SSLv3 tem algumas falhas de Segurança inerentes e pôde ser desabilitado em uma versão futura dos CRE. Especificamente, o Oracle estofamento na edição da vulnerabilidade da criptografia do legado Downgraded (CANICHE) (CVE-2014-3566) pode potencialmente conduzir a um escape dos dados criptografados a um atacante.

Embora uma correção de programa para esta vulnerabilidade seja aplicada aos CRE, a correção de programa exige que o server (CRE) e o cliente (seu navegador da Web) inclui-o. Se seu navegador da Web negocia SSLv3, é possível que não inclui a correção de programa.

Se você recebeu um alerta dos CRE que seu navegador usa SSLv3, seus dados criptografados puderam ser em risco. A fim evitar esta edição, Cisco recomenda que você promove a um navegador moderno com apoio do Transport Layer Security (TLS) como:

- Mozilla Firefox (alguma versão)
- Google Chrome (alguma versão)
- Internet explorer (versão 7 ou mais recente)
- Apple Safari (alguma versão)