Contenu

Introduction

Ce document décrit un avertissement au sujet de la Sécurité de votre connexion que vous pourriez rencontrer quand vous ouvrez une enveloppe chiffrée du service d'enveloppe recommandée de Cisco (CRES) ou visitez le site Web CRES si vous utilisez la version 3 de Secure Sockets Layer (SSLv3). Bien que vous puissiez encore accéder à l'enveloppe chiffrée et le site Web CRES, il est important que vous vous rendiez compte des risques de sécurité potentielle impliqués de l'utilisation de SSLv3 en votre navigateur.

Pourquoi recevez-vous un avertissement au sujet du cryptage SSLv3 sur CRES ?

Vous recevez l'avertissement parce que les serveurs CRES les ont détecté que votre navigateur Web a négocié une connexion SSLv3. Le protocole SSLv3 a quelques failles de sécurité inhérentes et pourrait être désactivé dans une version future de CRES. Spécifiquement, Oracle complétant récent sur Downgraded la vulnérabilité qu'existante de cryptage (CANICHE) (CVE-2014-3566) émettent peut potentiellement avoir comme conséquence une fuite des données cryptées à un attaquant.

Bien qu'un correctif pour cette vulnérabilité ait été appliqué à CRES, le correctif exige que le serveur (CRES) et le client (votre navigateur Web) l'incluent. Si votre navigateur Web négocie SSLv3, il est possible qu'il n'inclue pas le correctif.

Si vous receviez une alerte de CRES que votre navigateur utilise SSLv3, vos données cryptées pourraient être en danger. Afin d'éviter cette question, Cisco recommande que vous amélioriez à un navigateur moderne avec le support de Transport Layer Security (TLS) comme :

- Mozilla Firefox (toute version)
- Google Chrome (toute version)
- Internet Explorer (version 7 ou ultérieures)
- Apple Safari (toute version)