IEA FAQ: ¿Por qué usted recibe una advertencia sobre el cifrado SSLv3 en el servicio del sobre registrado de Cisco (CRE)?

Contenido

Introducción

Este documento describe una advertencia sobre la Seguridad de su conexión que usted puede ser que encuentre cuando usted abre un sobre cifrado registrado del servicio del sobre de Cisco (CRE) o visita el sitio web CRE si usted utiliza la versión 3 de Secure Sockets Layer (SSLv3). Aunque usted pueda todavía acceder el sobre cifrado y el sitio web CRE, es importante que usted es consciente de los riesgos de seguridad potencial implicados con el uso de SSLv3 en su navegador.

¿Por qué usted recibe una advertencia sobre el cifrado SSLv3 en los CRE?

Usted recibe la advertencia porque los servidores CRE detectaron que su buscador Web negoció una conexión SSLv3. El protocolo SSLv3 tiene algunos errores de seguridad inherentes y se pudo inhabilitar en una versión futura de los CRE. Específicamente, el Oracle reciente del relleno en el problema de la vulnerabilidad del cifrado de la herencia Downgraded (CANICHE) (CVE-2014-3566) puede potencialmente dar lugar a un escape de los datos encriptados a un atacante.

Aunque una corrección para esta vulnerabilidad se haya aplicado a los CRE, la corrección requiere que el servidor (CRE) y el cliente (su buscador Web) lo incluye. Si su buscador Web negocia SSLv3, es posible que no incluye la corrección.

Si usted recibió una alerta de los CRE que su navegador utiliza SSLv3, sus datos encriptados pudieron ser en peligro. Para evitar este problema, Cisco recomienda que usted actualiza a un navegador moderno con el soporte de Transport Layer Security (TLS) por ejemplo:

- Mozilla Firefox (cualquier versión)
- Google Chrome (cualquier versión)
- Internet Explorer (versión 7 o posterior)
- Apple Safari (cualquier versión)