IEA FAQ: Why do you receive a warning about SSLv3 encryption on Cisco Registered Envelope Service (CRES)?

TAC **Document ID: 118740**

Contributed by John Hess and Robert Sherwin, Cisco TAC Engineers.
Jan 15, 2015

Contents

Introduction

This document describes a warning about the security of your connection that you might encounter when you open a Cisco Registered Envelope Service (CRES) encrypted envelope or visit the CRES website if you use Secure Sockets Layer version 3 (SSLv3). Although you are still able to access the encrypted envelope and the CRES website, it is important that you are aware of the potential security risks involved with the use of SSLv3 in your browser.

Why do you receive a warning about SSLv3 encryption on CRES?

You receive the warning because CRES servers detected that your web browser negotiated an SSLv3 connection. The SSLv3 protocol has some inherent security flaws and might be disabled in a future version of CRES. Specifically, the recent Padding Oracle On Downgraded Legacy Encryption (POODLE) vulnerability (CVE−2014−3566) issue can potentially result in a leak of encrypted data to an attacker.

Although a patch for this vulnerability has been applied to CRES, the patch requires that both the server (CRES) and the client (your web browser) include it. If your web browser negotiates SSLv3, it is possible that it does not include the patch.

If you received an alert from CRES that your browser uses SSLv3, your encrypted data might be at risk. In order to avoid this issue, Cisco recommends that you upgrade to a modern browser with Transport Layer Security (TLS) support such as:

- Mozilla Firefox (any version)
- Google Chrome (any version)
- Internet Explorer (Version 7 or higher)
- Apple Safari (any version)