IEA FAQ: Waarom ontvangt u een waarschuwing over SSLv3-encryptie op Cisco Registered Service (CRES)?

Inhoud

Inleiding

Dit document beschrijft een waarschuwing voor de beveiliging van uw verbinding die u zou kunnen tegenkomen wanneer u een gecodeerde envelop van Cisco Registered Service (CRES) opent of de website van CRES bezoekt als u Secure Socket Layer versie 3 (SSLv3) gebruikt. Hoewel u nog steeds toegang hebt tot de gecodeerde envelop en de website van CRES, is het belangrijk dat u zich bewust bent van de potentiële veiligheidsrisico's die bij het gebruik van SSLv3 browser.

Waarom krijg je een waarschuwing over SSLv3 encryptie op CRES?

U ontvangt de waarschuwing omdat CRES-servers ontdekten dat uw webbrowser een SSLv3-verbinding tot stand heeft gebracht. Het SSLv3-protocol heeft een aantal inherente veiligheidsgebreken en kan in een toekomstige versie van CRES worden uitgeschakeld. Met name de recente kwestie van het opvullen van Oracle op gedowngraded Legacy Encryption (POODLE) kwetsbaarheid (CVE-2014-3566) kan mogelijk resulteren in een lek van gecodeerde gegevens aan een aanvaller.

Hoewel voor deze kwetsbaarheid een pleister is aangebracht op CRES, vereist de pleister dat zowel de server (CRES) als de client (uw webbrowser) deze opnemen. Als uw webbrowser over SSLv3 onderhandelt, is het mogelijk dat het niet de pleister bevat.

Als u een waarschuwing van CRES hebt ontvangen dat uw browser SSLv3 gebruikt, kan uw versleutelde gegevens in gevaar komen. Om deze kwestie te vermijden, adviseert Cisco u om aan een moderne browser met de steun van de Beveiliging van de Transport Layer (TLS) te verbeteren zoals:

- Mozilla Firefox (alle versies)
- Google Chrome (elke versie)
- Internet Explorer (versie 7 of hoger)
- Apple Safari (elke versie)