IEA FAQ:Cisco CRES(Registered Envelope Service)에서 SSLv3 암호화에 대한 경고가 표시되는 이유는 무엇입니까?

목차

소개

이 문서에서는 Cisco CRES(Registered Envelope Service) 암호화 엔벨로프를 열거나 SSLv3(Secure Sockets Layer 버전 3)을 사용하는 경우 CRES 웹 사이트를 방문할 때 발생할 수 있는 연결의 보안에 대한 경고를 설명합니다. 암호화된 엔벨로프와 CRES 웹 사이트에 계속 액세스할 수 있지만 브라우저에서 SSLv3을 사용하는 것과 관련된 잠재적인 보안 위험을 알고 있어야 합니다.

CRES에서 SSLv3 암호화에 대한 경고가 표시되는 이유는 무엇입니까?

CRES 서버가 웹 브라우저에서 SSLv3 연결을 협상한 것을 감지했기 때문에 경고가 표시됩니다 .SSLv3 프로토콜에는 내재된 보안 결함이 있으며 향후 CRES 버전에서 비활성화될 수도 있습니다 .특히 최근 Padding Oracle On Downgraded Legacy Encryption (POODLE) 취약성 (CVE-2014-3566) 문제는 잠재적으로 공격자에게 암호화된 데이터가 유출될 수 있습니다.

이 취약성에 대한 패치가 CRES에 적용되었지만 패치에는 서버(CRES)와 클라이언트(웹 브라우저)에 모두 포함되어야 합니다.웹 브라우저에서 SSLv3을 협상하는 경우 패치가 포함되지 않을 수 있습니다.

브라우저에서 SSLv3을 사용한다는 경고를 CRES로부터 받은 경우 암호화된 데이터가 위험에 노출될 수 있습니다.이러한 문제를 방지하기 위해 다음과 같은 TLS(Transport Layer Security)가 지원되는 최신 브라우저로 업그레이드할 것을 권장합니다.

- Mozilla Firefox(모든 버전)
- Google Chrome(모든 버전)
- Internet Explorer(버전 7 이상)
- Apple Safari(모든 버전)