

# IEA FAQ : 为什么收到关于SSLv3加密的一警告在思科注册信封服务(茨雷斯岛) ?

## 目录

### [简介](#)

[为什么收到关于SSLv3加密的一警告在茨雷斯岛 ?](#)

## 简介

本文描述关于您的连接安全的一警告您也许遇到，当您开始Cisco注册的信封服务(CRES)时加密信封或访问[CRES网站](#)，如果使用安全套接字协议层版本3 (SSLv3)。虽然您能访问已加密信封和茨雷斯岛网站，重要的是您知道潜在的安全风险涉及与使用SSLv3在您的浏览器。

## 为什么收到关于SSLv3加密的警告在茨雷斯岛 ?

您收到警告，因为茨雷斯岛服务器检测您的Web浏览器协商SSLv3连接。SSLv3协议在茨雷斯岛未来版本有一些内在的安全漏洞，并且也许禁用。特别地，在Downgraded传统加密(长卷毛狗)漏洞([CVE-2014-3566](#))问题的最近的填充的Oracle能潜在导致已加密数据泄漏到攻击者。

虽然此漏洞的一补丁程序应用到茨雷斯岛，补丁程序要求服务器(茨雷斯岛)，并且客户端(您的Web浏览器)包括它。如果您的Web浏览器协商SSLv3，很可能，不包括补丁程序。

如果接收从茨雷斯岛的一警报您的浏览器使用SSLv3，您的已加密数据也许是危险的危险。为了避免此问题，思科建议您升级到有传输层安全(TLS)支持的一个现代浏览器例如：

- [Mozilla Firefox](#) (任何版本)
- [谷歌镀铬物](#) (任何版本)
- [Internet Explorer](#) (版本7或以上)
- [苹果公司Safari](#) (任何版本)