了解和排除无线客户端上的HTTPS Web身份验证证书不信任行为

目录

简介

本文档介绍在对Web浏览器处理安全套接字层(SSL)证书的方式进行更改后，无线客户端连接到第3层身份验证无线局域网(WLAN)时的行为。

先决条件

要求

Cisco 建议您了解以下主题：

- 超文本传输协议安全(HTTPS)。
- SSL证书。
- 思科无线局域网控制器(WLC)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Chrome Web浏览器版本74.x或更高版本。
- Firefox Web浏览器版本66.x或更高版本。
- 思科无线局域网控制器8.5.140.0或更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

超文本传输协议 (HTTP)Internet上网站的流量不安全，可能被意外的人拦截和处理。因此，为了实施SSL/TLS加密等构成HTTPS的额外安全措施，必须增加对敏感应用的HTTP使用。

HTTPS需要使用 SSL 证书，用于验证网站的身份并允许在web服务器和终端浏览器之间建立安全连接。SSL证书必须由浏览器和操作系统的受信任CA根证书列表中包含的受信任证书颁发机构(CA)颁发。

最初，SSL证书使用安全散列算法第1版(SHA-1)，该版本使用160位散列。但是，由于各种缺点，SHA-1逐渐被SHA-2取代，SHA-2是一组长度不同的散列算法，其中最常用的是256位。

问题

不可信证书的常见场景

Web浏览器不信任SSL证书的原因有几个，但最常见的原因是：

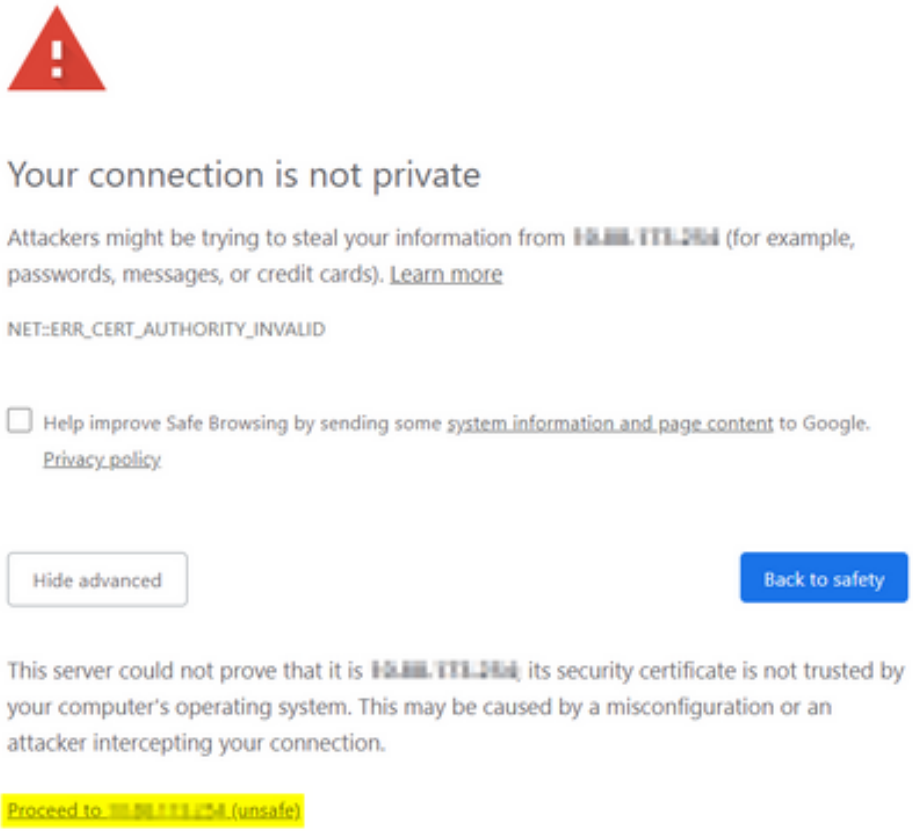
- 证书不是由受信任证书颁发机构颁发的（证书是自签名的，或者在内部CA的情况下客户端未安装根CA证书）。
- 证书的公用名(CN)或使用者备用名(SAN)字段与为导航到此站点而输入的统一资源定位器(URL)不匹配。
- 证书已过期或客户端时钟配置错误（在证书有效期外）。
- 中间CA或设备证书（如果没有中间CA）正在使用SHA-1算法。

以前的行为

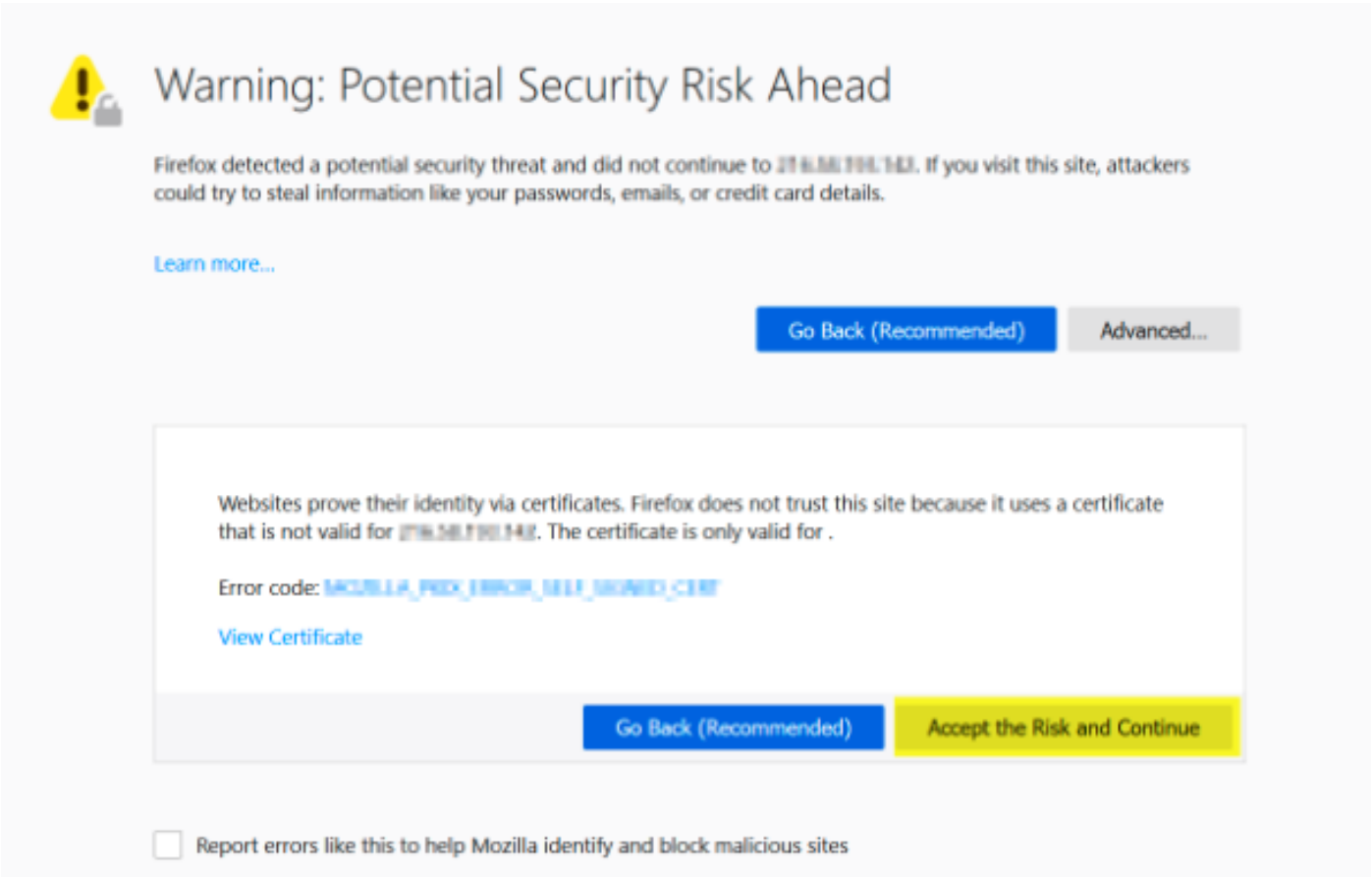
当早期版本的Web浏览器检测到设备证书不可信时，会提示安全 预警 （每个浏览器上的文本和外观各不相同）。 安全性 预警 要求用户接受安全风险并继续访问目标网站，或拒绝连接。 接受后 用户获得最终用户到目标强制网络门户的重定向行为的风险：

> **注意：**要继续的操作可隐藏在特定浏览器的“高级选项”下。

低于74的Google Chrome版本显示警报，如图所示：



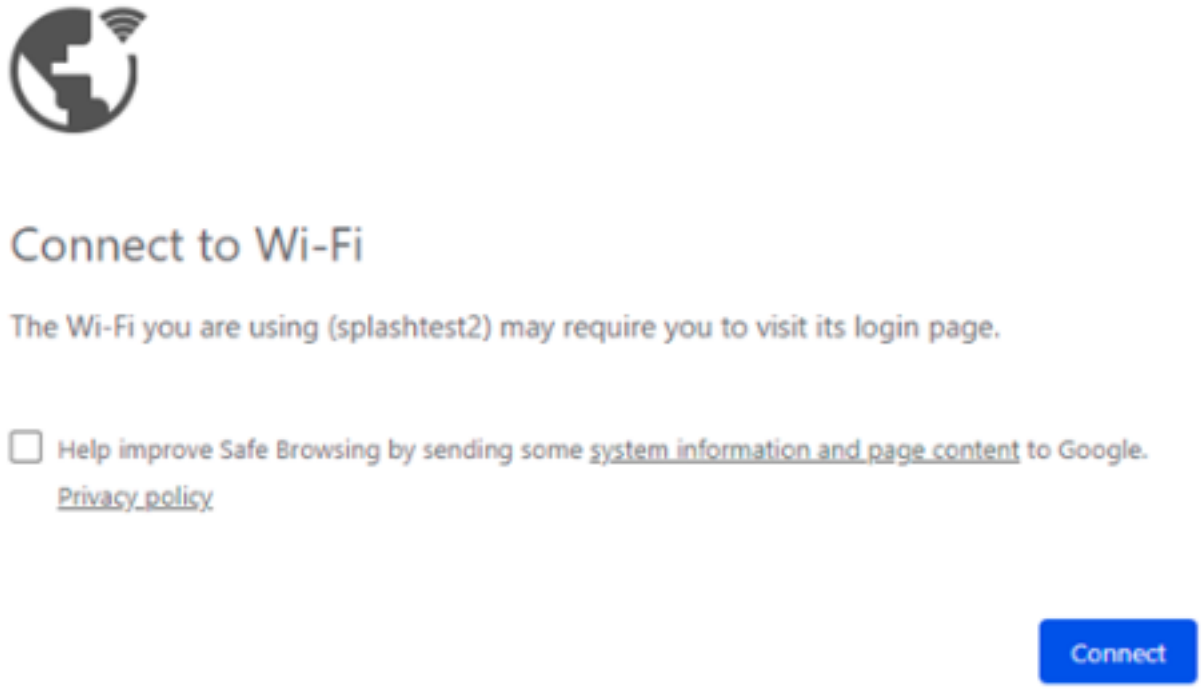
低于66的Mozilla Firefox版本显示警报，如图所示：



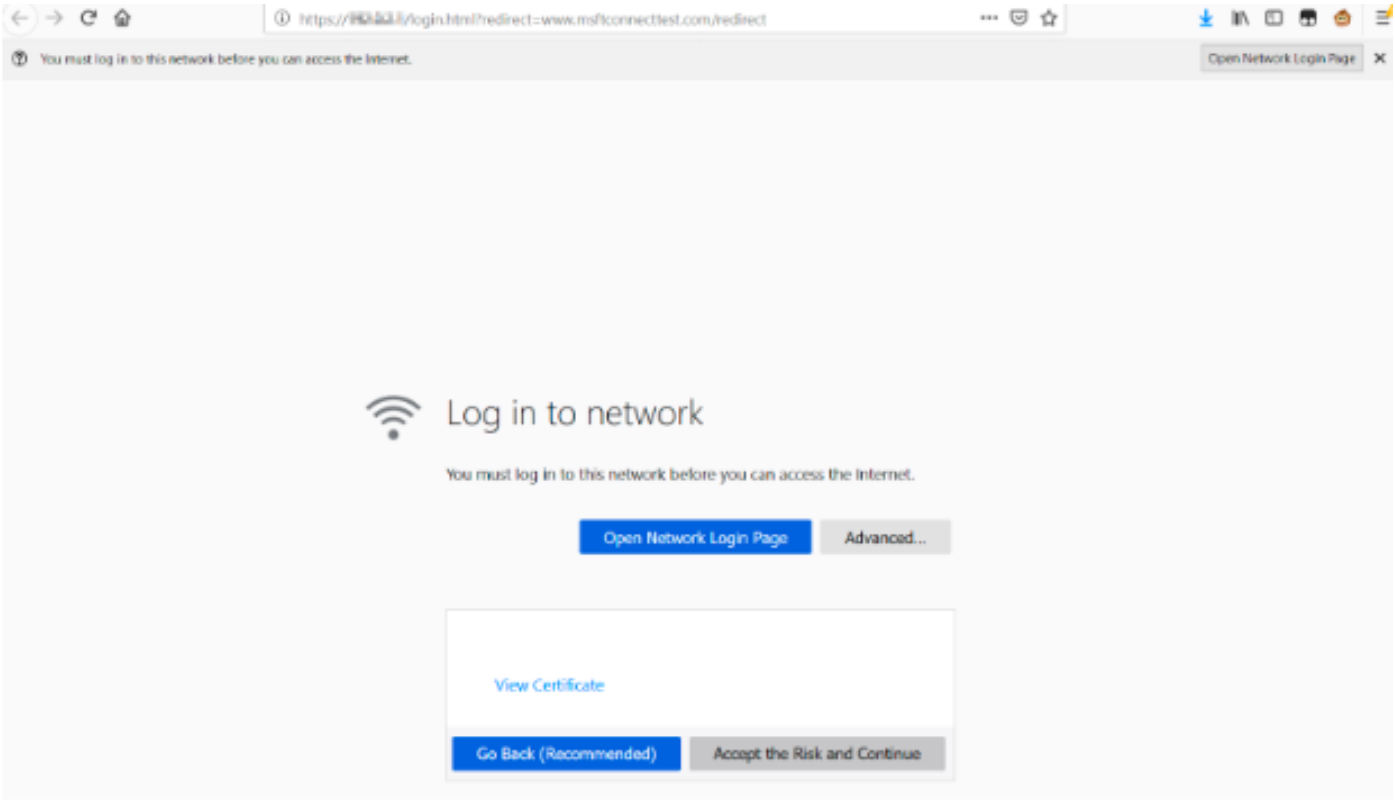
更改的行为

Google Chrome和Mozilla Firefox等一些网络浏览器通过证书验证改变了处理安全连接的方式。Google Chrome（74.x及更高版本）和Mozilla Firefox（66.x及更高版本）要求浏览器先向外部URL发送无条件请求 用户可以浏览强制网络门户。但是，此请求被无线控制器拦截，因为所有流量在到达最终连接状态之前都会被拦截。请求 然后 启动到强制网络门户的新重定向 创建 由于用户 无法 请参阅门户。

Google Chrome 74.x及更高版本显示警报：**连接到Wi-Fi您使用的Wi-Fi可能需要您访问其登录页**，如图所示：



Mozilla Firefox 66.x及更高版本显示警报：**登录网络您必须登录此网络才能访问Internet，如图**所示：



此页包含"接**受风险并继续**"选项。但是，当选择此选项时，会创建具有相同信息的新选项卡。

> **注意**：此文档漏洞由ISE团队提交，作为客户的外部参考：CSCvj04703 - Chrome:访客/BYOD门户上的重定向流在ISE门户上被不受信任的证书中断。

解决方案

内部网络身份验证的解决方法（WLC的内部网络登录页）

第 1 项

在WLC上禁用WebAuth SecureWeb。由于问题是由证书验证创建HTTPS安全机制引起的， 使用HTTP，跳过证书验证并允许客户端呈现强制网络门户。

要在WLC上禁用WebAuth SecureWeb，可以运行以下命令：

```
config network web-auth secureweb disable
```

> **注意**：必须重新启动WLC，更改才能生效。

第 2 项

使用备用Web浏览器。到目前为止，这个问题被Google Chrome和Mozilla Firefox隔离；因此，Internet Explorer、Edge和本机Android Web浏览器等浏览器不显示此行为，可用于访问强制网络门户。

外部Web身份验证的解决方法

第 1 项

由于网络身份验证过程的这种变化允许通过预身份验证访问列表进行通信控制，因此可以添加例外，以便用户可以继续访问强制网络门户。此类例外通过URL访问列表完成(从AireOS版本8.3.x开始支持集中WLAN和8.7.x支持FlexConnect本地交换WLAN)。 URL可能取决于Web浏览器，但已识别为 http://www.gstatic.com/ Google Chrome和 http://detectportal.firefox.com/ Mozilla Firefox。

永久性修正

为了解决此问题，建议在WLC中安装由受信任证书颁发机构颁发的带SHA-2算法的WebAuth SSL证书。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- **生成第三方证书的CSR并且下载被串连的证书到WLC**
- **Google Chrome隐私白皮书**
- **技术支持和文档 - Cisco Systems**