HTTPS WebVerificatie certificaat wangedrag bij draadloze clients begrijpen en probleemoplossing

Inhoud

Inleiding

Dit document beschrijft het gedrag van draadloze klanten wanneer ze verbinding maken met een Layer 3 verificatie Wireless Local Area Network (WLAN) na wijzigingen die zijn aangebracht op de manier waarop webbrowsers Secure Socket Layer (SSL)-certificaten afhandelen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- HyperText Transfer Protocol (HTTPS).
- SSL-certificaten.
- Cisco draadloze LAN-controller (WLC).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Chrome web browser versie 74.x of hoger.
- Firefox webbrowser versie 6.x of hoger.
- Cisco draadloze LAN-controller versie 8.5.14.0 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Hypertext Transfer Protocol (HTTP) het internetverkeer is niet veilig en kan door onbedoelde personen worden onderschept en verwerkt. Daarom is een groter gebruik van HTTP voor gevoelige toepassingen nodig om extra beveiligingsmaatregelen te nemen als SSL/TLS-encryptie, die HTTPS vormt.

HTTPS vereist het gebruik van SSL certificaten om de identiteit van een website te valideren en een beveiligde verbinding tussen de webserver en de browser van het eindpunt mogelijk te maken. SSL-certificaten moeten worden afgegeven door een vertrouwde certificeringsinstantie (CA) die is opgenomen in de lijst van vertrouwde CA-basiscertificaten van browsers en besturingssystemen.

Eerst gebruikte SSL-certificaten Secure Hashing Algorithm versie 1 (SHA-1), die een 160-bits hash gebruikt. Door een verscheidenheid aan zwakheden is SHA-1 echter geleidelijk vervangen door SHA-2, een groep hashing-algoritmen met verschillende lengte tussen waarvan de populairste 256 bit is.

Probleem

Gemeenschappelijke scenario's voor onvertrouwde certificaten

Er zijn verschillende redenen voor een webbrowser om geen SSL-certificaat te vertrouwen, maar de meest voorkomende redenen zijn:

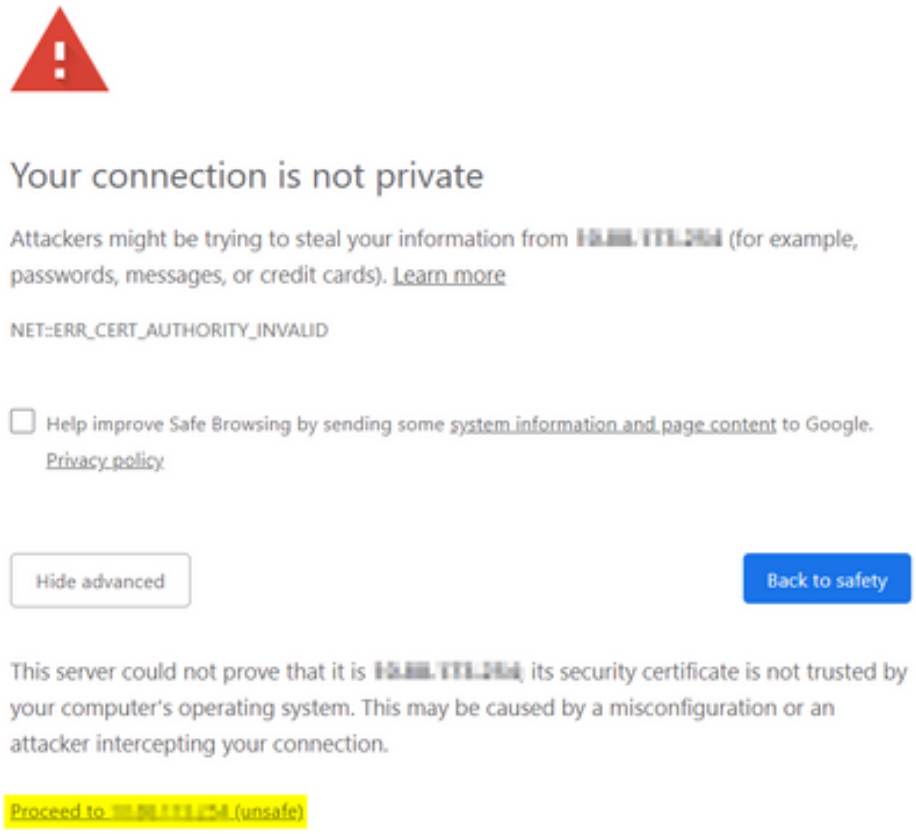
- Het certificaat wordt niet afgegeven door een vertrouwde certificeringsinstantie (het certificaat is zelf ondertekend of de klant heeft het basiscertificaat niet geïnstalleerd in het geval van interne CA).
- De velden Gemeenschappelijke Naam (CN) of Onderwerp Alternate Name (SAN) van het certificaat komen niet overeen met de URL (Uniform Resource Locator) die is ingevoerd om naar deze site te navigeren.
- Het certificaat is verlopen of de klok op de cliënt is onjuist ingesteld (buiten de geldigheidsduur van het certificaat).
- SHA-1 algoritme wordt gebruikt door de intermediaire CA, of het apparaatcertificaat (voor het geval dat er geen intermediaire CA is).

Eerder gedrag

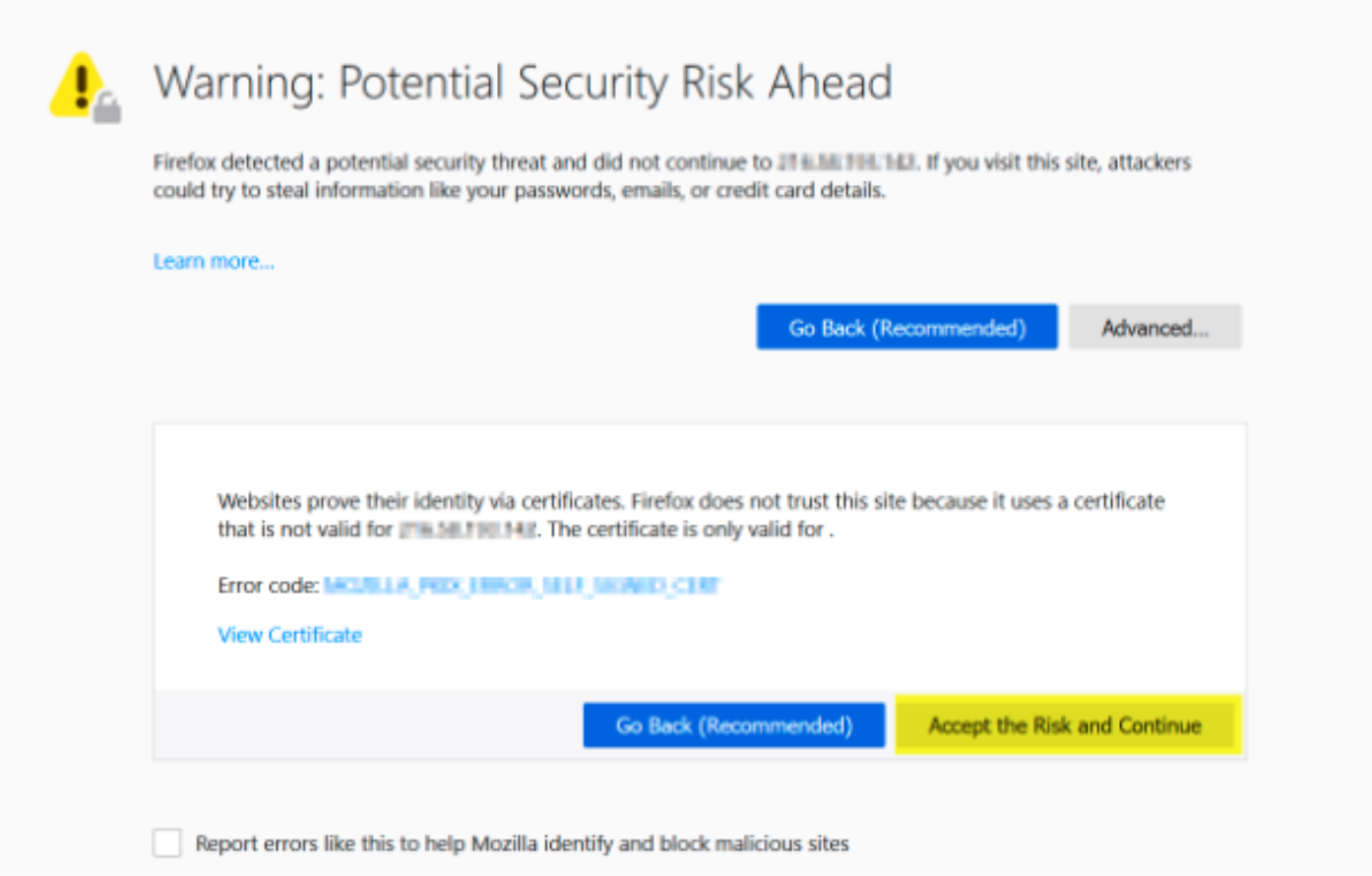
Wanneer eerdere versies van webbrowsers een apparaatcertificaat als onbetrouwbaar herkennen, worden ze tot een beveiliging gewend waarschuwen (tekst en weergave variëren per browser). De beveiliging waarschuwen vraagt de gebruiker om het beveiligingsrisico te accepteren en door te gaan naar de geplande website, of de verbinding te weigeren. Na aanvaarding van het risico dat de gebruiker het omrichtingsgedrag van de eindgebruiker naar het beoogde portaal in gevangenschap doorvoert:

> **Opmerking:** De actie om verder te gaan, kan onder Geavanceerde opties op specifieke browsers worden verborgen.

Google Chrome-versies van minder dan 74 tonen de waarschuwing zoals in de afbeelding getoond:



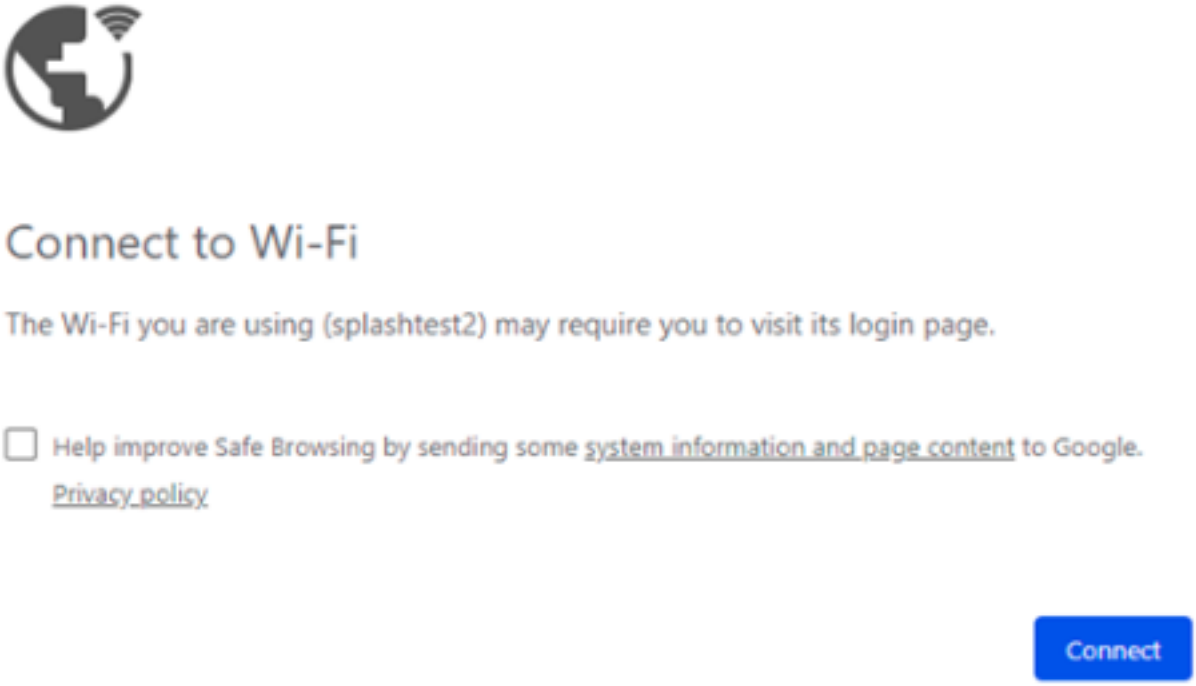
Mozilla Firefox-versies lager dan 66 tonen het alarm zoals in de afbeelding:



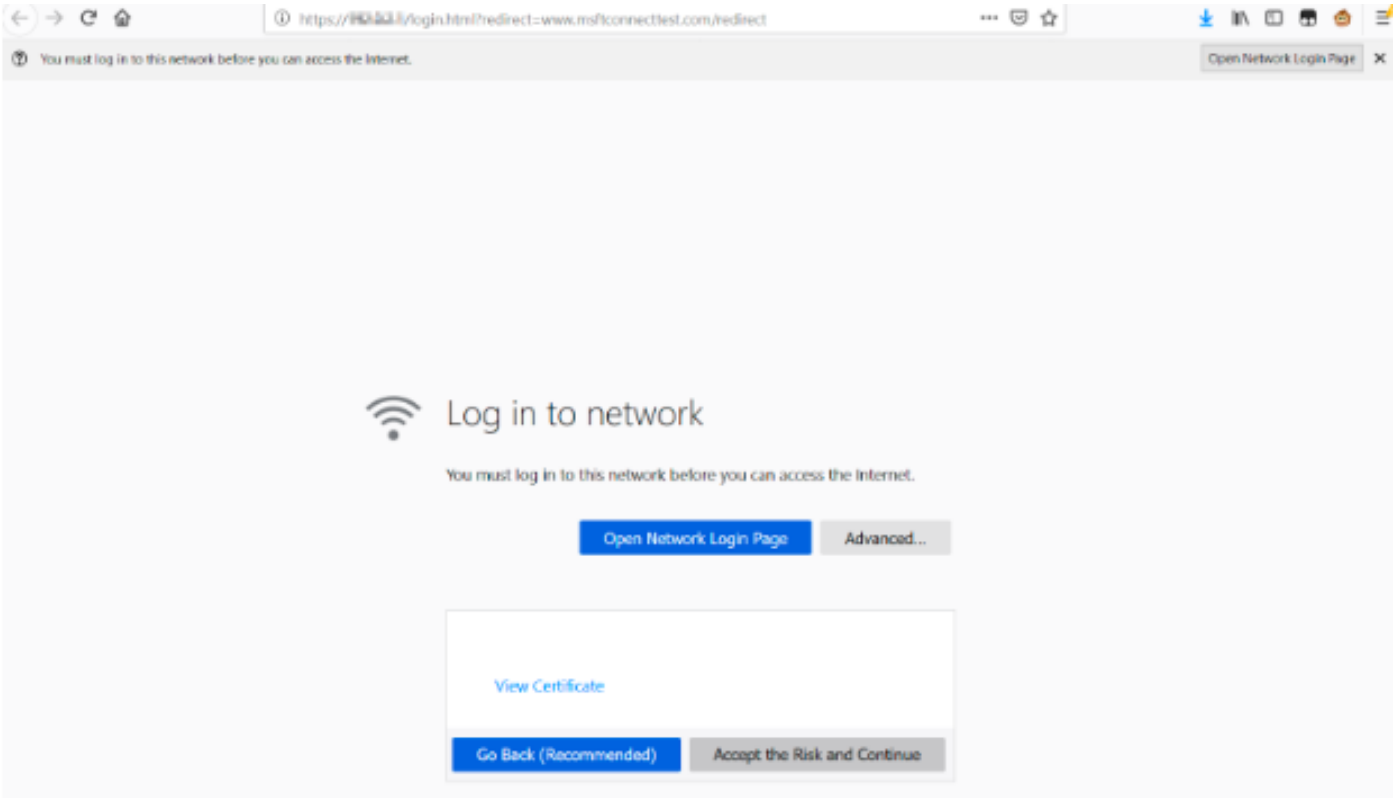
Gewijzigd gedrag

Sommige webbrowsers als Google Chrome en Mozilla Firefox veranderden de manier waarop ze met veilige verbindingen omgaan door middel van certificatencontrole. Google Chrome (74.x en hoger) en Mozilla Firefox (66.x en hoger) eisen dat de browser een kosteloos verzoek aan externe URL's stuurt voordat de gebruiker kan naar het portaal in gevangenschap bladeren. Dit verzoek wordt echter tegengehouden door de draadloze controller omdat al het verkeer geblokkeerd is voordat de uiteindelijke verbindingsstaat kan worden bereikt. Het verzoek dan start een nieuwe omleiding naar het portaal in gevangenschap die een omleidingslus sinds de gebruiker niet in staat is zie het portaal.

Google Chrome 74.x en hoger geeft het alarm: **Connect met Wi-Fi De Wi-Fi die u gebruikt, kan vereisen dat u de logpagina bezoekt**, zoals in de afbeelding wordt getoond:



Mozilla Firefox 66.x en hoger geeft de waarschuwing weer: **Aanmelden met om netwerk U moet aan dit netwerk loggen voordat u toegang tot internet kunt krijgen**, zoals in de afbeelding:



Deze pagina bevat een **optie Risico accepteren en doorgaan**. Wanneer deze optie echter is geselecteerd, wordt er een nieuw tabblad met dezelfde informatie gemaakt.

> **Opmerking:** Dit documentatiebug werd door het ISE-team ingediend als een externe referentie voor klanten:CSCvj04703 - Chrome: De omleiding van stroom op gastarts-/BYOD-portal is verbroken met een onbetrouwbaar certificaat op een ISE-portal.

Oplossing

Workround for Interne Web-Auth (WLC's interne weblogpagina)

Optie 1

Schakel Webex Secure Web in via de WLC. Aangezien de afgifte wordt veroorzaakt door de validering van certificaten om het HTTPS-beveiligingsmechanisme in te stellen, gebruiken HTTP om de certificatie-validatie over te slaan en klanten toe te staan om het portaal in gevangenschap weer te geven.

U kunt Webex Secure Web in WLC uitschakelen door deze opdracht te starten:

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

Opmerking: U moet de WLC opnieuw opstarten voordat de wijziging van kracht wordt.

Optie 2

Gebruik alternatieve webbrowsers. De kwestie is tot nu toe geïsoleerd geraakt aan Google Chrome en Mozilla Firefox; Daarom presenteren browsers als Internet Explorer, Edge en native Android-webbrowsers dit gedrag niet en kunnen ze worden gebruikt om het portal te openen.

Workround voor extern web-auth

Optie 1

Aangezien deze wijziging van het webauthenticatieproces communicatiecontrole mogelijk maakt via de toegangslijst voor de verificatie, kan een uitzondering worden toegevoegd zodat de gebruikers naar het interne portaal kunnen blijven. Zulke uitzonderingen worden gemaakt via URL-toegangslijsten (ondersteuning start op AireOS-versies 8.3.x voor gecentraliseerde WLAN's en 8.7.x voor FlexConnect Local Switching WLAN's). De URL's kunnen afhankelijk zijn van webbrowsers, maar zij zijn geïdentificeerd als http://www.gstatic.com/ voor Google Chrome en http://detectportal.firefox.com/ voor Mozilla Firefox.

Permanent Fix

Om dit probleem op te lossen, wordt het aanbevolen om een WebAuth SSL certificaat met SHA-2 algoritme te installeren, dat door een vertrouwde certificaatautoriteit, in het WLC wordt verstrekt.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- CSR genereren voor certificaten van derden en opgeslagen certificaten downloaden bij de WLC
- Google Chrome Privacy Whitepaper
- Technische ondersteuning en documentatie – Cisco Systems