Problemas de confianza de CA personalizada de Secure Access con Firefox y Safari en macOS

Contenido

Problema

Los usuarios experimentaron errores de certificados de confianza en los navegadores macOS (Safari y Firefox) al acceder al tráfico de Internet descifrado a través de Cisco Secure Access. El navegador Chrome funcionaba correctamente, pero Safari y Firefox mostraban advertencias de "certificado no fiable" y bloqueaban el acceso a sitios web y aplicaciones.

La cadena completa de certificados mostraba:

- Sitio web (como cnn.com) > Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

Los navegadores Firefox y Safari detuvieron la validación de certificados en los certificados intermedios de Cisco y no pudieron encadenarse a la CA raíz, mientras que Chrome validó correctamente toda la cadena de certificados.

Entorno

- Implementación de Cisco Secure Access con autoridad de certificados personalizada para el descifrado HTTPS
- dispositivos macOS con navegadores Safari y Firefox
- Infraestructura de certificados de CA personalizada con Microsoft Certificate Authority
- Políticas de acceso a Internet con el descifrado y la prevención de intrusiones habilitados
- ID de organización: xxxxx

Resolución

El problema se resolvió identificando una discordancia de codificación en la cadena de certificados y cambiando a la CA raíz de Cisco Secure Access para el descifrado.

Análisis de causa raíz

El equipo identificó que la entidad de certificación personalizada se creó mediante la codificación de cadenas imprimibles, lo que causó problemas de incompatibilidad incluso cuando los certificados de hoja se establecieron en UTF8STRING. Firefox y Safari requieren que todos los certificados de una cadena estén en el mismo formato, mientras que Chrome no tiene este requisito estricto.

Pasos de resolución

Cambiar a CA raíz de Cisco Secure Access

Soluciones alternativas

Si se requiere el uso de una CA personalizada, se identificaron estas opciones:

- Reconstruir toda la infraestructura de certificados mediante la codificación UTF8 (alto impacto, no recomendado)
- Utilizar una infraestructura de certificados diferente que admita la codificación UTF8
- La limitación de Firefox y Safari no puede funcionar con la configuración de CA personalizada actual

Causa

La causa raíz fue una discordancia de codificación entre Microsoft Certificate Authority (que utiliza la codificación printablstring de forma predeterminada) y la cadena UTF8 utilizada por Cisco Secure Access. Firefox y Safari tienen requisitos de validación de certificados más estrictos y necesitan que todos los certificados de la cadena utilicen una codificación coherente. la validación más indulgente en Chrome le permitió trabajar con la cadena de codificación mixta, mientras que Firefox y Safari rechazaron los formatos de certificado incoherentes.

La entidad emisora de certificados de Microsoft creó certificados mediante la codificación printablstring, pero los certificados intermedios de Cisco Secure Access utilizaron la codificación UTF8STRING. Esta discordancia hizo que Firefox y Safari fallaran en la validación de la cadena de certificados en el nivel de certificado intermedio de Cisco.

Contenido relacionado

- Configuración de Webex Meeting Access en SWG
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).