Problemi di trust tra CA personalizzati per Secure Access con Firefox e Safari su macOS

Sommario

Problema

Gli utenti hanno riscontrato errori di attendibilità dei certificati nei browser macOS (Safari e Firefox) quando accedono al traffico Internet decrittografato tramite Cisco Secure Access. Il browser Chrome funzionava correttamente, ma Safari e Firefox hanno visualizzato avvisi di "certificato non attendibile" e bloccato l'accesso a siti web e applicazioni.

L'intera catena di certificati ha mostrato:

- Sito Web (ad esempio cnn.com) > Cisco Secure Access Custom CA > Cisco Secure Access Custom R3 CA > Cisco Secure Access Custom CA > xxxx-SUBCA1 > xxxxROOT-CA

I browser Firefox e Safari hanno interrotto la convalida dei certificati ai certificati intermedi Cisco e non sono riusciti a concatenarsi alla CA radice, mentre Chrome ha convalidato l'intera catena di certificati.

Ambiente

- Distribuzione Cisco Secure Access con Autorità di certificazione personalizzata per la decrittografia HTTPS
- dispositivi macOS con browser Safari e Firefox
- Infrastruttura personalizzata dei certificati CA tramite Microsoft Certificate Authority
- Criteri di accesso a Internet con decrittografia e prevenzione delle intrusioni attivate
- ID organizzazione: xxxxx

Risoluzione

Il problema è stato risolto identificando una mancata corrispondenza di codifica nella catena di certificati e passando alla CA radice di accesso sicuro Cisco per la decrittografia.

Analisi della causa principale

Il team ha identificato che l'autorità di certificazione personalizzata è stata creata utilizzando la codifica di stringa stampabile, che ha causato problemi di incompatibilità anche quando i certificati foglia erano impostati su UTF8STRING. Firefox e Safari richiedono che tutti i certificati in una catena siano nello stesso formato, mentre Chrome non ha questo requisito rigoroso.

Fasi risoluzione

Passa alla CA radice di accesso sicuro Cisco

Soluzioni alternative

Se è necessario utilizzare una CA personalizzata, sono state identificate le opzioni seguenti:

- Ricostruire l'intera infrastruttura dei certificati utilizzando la codifica UTF8 (impatto elevato, scelta non consigliata)
- Usa un'infrastruttura di certificati diversa che supporta la codifica UTF8
- Limitazione di Firefox e Safari non può funzionare con l'impostazione CA personalizzata corrente

Causa

La causa principale è una mancata corrispondenza di codifica tra Microsoft Certificate Authority (che per impostazione predefinita utilizza la codifica printablestring) e la catena UTF8 utilizzata da Cisco Secure Access. Firefox e Safari hanno requisiti di convalida dei certificati più severi e richiedono tutti i certificati nella catena per utilizzare una codifica coerente. la convalida più indulgente in Chrome ha permesso di lavorare con la catena di codifica mista, mentre Firefox e Safari hanno rifiutato i formati di certificato incoerenti.

La CA Microsoft ha creato i certificati utilizzando la codifica printablestring, ma i certificati intermedi Cisco Secure Access utilizzano la codifica UTF8STRING. A causa di questa mancata corrispondenza, Firefox e Safari non sono in grado di convalidare la catena di certificati a livello di certificato intermedio Cisco.

Contenuto correlato

- Configurazione dell'accesso a Webex Meeting in SWG
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).