Risoluzione dei problemi relativi alla scadenza dei certificati durante l'accesso di Umbrella Integration

Sommario

Introduzione

In questo documento viene descritto come risolvere un errore di scadenza di un certificato quando un'integrazione Umbrella accede a s-platform.api.opendns.com o fireeye.vendor.api.opendns.com.

Problema

Le integrazioni Umbrella che utilizzano client di terze parti possono non riuscire con un errore nella verifica del certificato digitale del server per le API Umbrella all'indirizzo s-platform.api.opendns.com and fireeye.vendor.api.opendns.com. Il testo o il codice dell'errore varia a seconda del programma client utilizzato nell'integrazione, ma in genere indica che è presente un certificato scaduto.

Causa

Il problema non è causato dal certificato del server, attualmente valido. Il problema è invece causato da un archivio certificati attendibile non aggiornato utilizzato dal client.

Il server Web che serve s-platform.api.opendns.com e fireeye.vendor.api.opendns.com utilizza un certificato digitale rilasciato (firmato digitalmente) dal certificato intermedio R3 dall'autorità di certificazione Let's Encrypt. R3 è firmato da una chiave pubblica che si trova sia nel Certificato radice SRG X1 di Let's Encrypt e una versione precedente con firma incrociata di SRG Root X1. Esistono pertanto due percorsi di convalida: uno che termina alla radice SRG X1 corrente e uno che termina all'autorità emittente della versione con firma incrociata, il certificato DST Root CA X3, rilasciato dall'autorità di certificazione IdenTrust.

Un diagramma del problema è disponibile in Crittografia. Inoltre, lo strumento Qualys SSL Labs può essere utilizzato per visualizzare i due "percorsi di certificazione" con i rispettivi certificati e i dettagli del certificato, ad esempio le date di scadenza.

I certificati radice vengono conservati in uno o più archivi certificati attendibili nei sistemi client. Il 30 settembre 2021, il certificato X3 della CA radice DST è scaduto. A partire da questa data, i client che dispongono del certificato X3 della CA radice dell'origine della distribuzione nel proprio archivio attendibile, ma non dispongono del certificato radice X1 dell'origine dell'origine dell'aggregazione dei cluster più recente, non riescono a connettersi a s-platform.api.opendns.com o fireeye.vendor.api.opendns.com a causa di un errore del certificato. Il messaggio di errore o il codice può indicare un certificato scaduto come motivo dell'errore. Il certificato scaduto è il certificato X3 della CA radice dell'installazione remota presente nell'archivio dei trust del client, non il certificato del server per i server API, s-platform.api.opendns.com e fireeye.vendor.api.opendns.com.

Risoluzione

Per risolvere il problema, aggiornare l'archivio di attendibilità del client per includere il nuovo certificato SRG Root X1, che può essere scaricato dal sito Web di Let's Encrypt. (Questa pagina fornisce anche siti Web per testare i client.) Consultare la documentazione del client o del sistema operativo per ottenere istruzioni sulla visualizzazione e l'aggiornamento dell'archivio di attendibilità del client. Se è disponibile un pacchetto di aggiornamento ufficiale o un meccanismo di aggiornamento automatico, è in genere preferibile all'aggiornamento manuale dell'archivio attendibile.

Se si aggiorna manualmente l'archivio di attendibilità con il nuovo certificato X1 radice SRG, è consigliabile rimuovere anche il certificato X3 radice DST scaduto, nel caso in cui il codice di generazione del percorso di convalida del client sia problematico. Un aggiornamento ufficiale dell'archivio di attendibilità da parte del provider del client o del sistema operativo in uso può aggiungere la radice SRG X1 e rimuovere il certificato X3 della CA radice dell'origine DST.

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).