Risoluzione dei problemi "517 Upstream Certificate Revoked"

Sommario

Introduzione

In questo documento viene descritto come risolvere il problema relativo all'errore "Certificato upstream 517 revocato" quando si passa a un URL HTTPS.

Problema

Quando il proxy Web Umbrella Secure Web Gateway (SWG) è configurato per eseguire l'ispezione HTTPS, un utente può ricevere una pagina di errore Certificato upstream revocato 517. Questo errore indica che il sito Web richiesto ha inviato un certificato digitale nella negoziazione TLS con stato "revocato" in base all'emittente del certificato o a un'autorità analoga. Un certificato revocato non è più valido.

13351060307092

Causa

Quando un client Umbrella effettua una richiesta HTTPS tramite Umbrella Secure Web Gateway, SWG esegue i controlli di revoca dei certificati utilizzando il protocollo OCSP (Online Certificate Status Protocol). OCSP fornisce lo stato di revoca di un certificato. SWG effettua richieste OCSP per lo stato di revoca dei certificati per conto dei client Umbrella.

SWG determina lo stato di revoca del certificato del server Web richiesto e di tutti i certificati intermedi emittenti nel percorso di un certificato radice attendibile. Questi controlli garantiscono che una catena di attendibilità valida non sia più valida dopo il rilascio.

In un certificato digitale che utilizza la verifica delle revoche OCSP, l'estensione "Authority Information Access" X.509 contiene uno o più campi "OCSP". Un campo contiene un URL HTTP per un "endpoint" OCSP (server Web) a cui è possibile richiedere lo stato di revoca del certificato. SWG effettua richieste a ciascun URL OCSP in un certificato finché non riceve una risposta che indica uno dei seguenti elementi:

- il certificato è valido (non revocato) e in quel momento il gruppo SWG consente alla richiesta Web di procedere, OPPURE
- un'azione diversa da una risposta "certificato valido" OCSP (ad esempio, il certificato viene revocato, il server non è in grado di rispondere al momento, uno stato di errore HTTP, un timeout del livello di rete/trasporto e così via) in cui SWG presenta la pagina/il messaggio di errore appropriato e la richiesta Web non riesce

Si noti che le risposte OCSP vengono in genere memorizzate nella cache e utilizzate per

rispondere a controlli futuri. Il tempo di memorizzazione nella cache viene impostato dal server nella risposta OCSP.

Comportamento diverso durante l'esplorazione diretta

I client Web possono utilizzare diversi meccanismi di verifica delle revoche, a seconda del client. Per impostazione predefinita, ad esempio, il browser Chrome di Google non utilizza né il metodo OCSP né il metodo CRL standard. Al contrario, Chrome utilizza una versione proprietaria di un CRL chiamato CRLSet, che Secure Web Gateway non utilizza. Di conseguenza, Chrome potrebbe non produrre lo stesso risultato di SWG quando si controlla lo stato di revoca di un certificato.

Si noti tuttavia che, come afferma la documentazione di CRLSet, "in alcuni casi, la libreria dei certificati di sistema sottostante esegue sempre questi controlli indipendentemente da Chromium." Pertanto, a seconda dell'ambiente locale, un controllo OCSP e/o CRL può essere eseguito dal browser o dalle librerie del servizio di crittografia del sistema operativo, ad esempio SChannel, Secure Transport o NSS.

Si noti inoltre che non è garantito che i controlli OCSP e CRL producano lo stesso risultato.

Consultare la documentazione del browser o del sistema operativo per determinare quali controlli di revoca dei certificati vengono eseguiti dai client durante l'esplorazione.

Risoluzione

L'utilizzo di certificati validi è responsabilità dell'amministratore del server Web. La correzione dei certificati revocati deve essere eseguita sul server dall'amministratore del server. Cisco Umbrella non può assistere in questo processo.

Cisco Umbrella sconsiglia vivamente di accedere a un sito Web che usa un certificato revocato. Le soluzioni alternative possono essere utilizzate solo quando l'utente comprende appieno il motivo per cui un sito utilizza un certificato revocato e accetta pienamente eventuali rischi.

Per evitare l'errore, è possibile esentare il sito dall'ispezione HTTPS creando un elenco di decrittografia selettiva che include il nome di dominio del sito. L'Elenco decrittografia selettiva verrà applicato al criterio Web che consente l'accesso al sito. In alternativa, è possibile aggiungere il sito all'elenco dei domini esterni per inviare il traffico direttamente al sito, ignorando SWG.

Ulteriori informazioni

I clienti che desiderano confermare la revoca del certificato di un server possono utilizzare strumenti di terze parti progettati per controllare lo stato della revoca. In particolare, lo strumento di test server SSL di Qualys SSL Labs esegue i controlli OCSP e CRL, oltre a fornire altre informazioni sulla validità dei certificati. Lo strumento è disponibile online all'indirizzo:

- https://www.ssllabs.com/ssltest/analyze.html

Si consiglia di utilizzare questo strumento per controllare il sito che genera un errore 517 Upstream Certificate Revoked, prima di aprire una richiesta di assistenza in Cisco Umbrella.

Vedere anche: https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors

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).