Comprendere gli errori comuni dei certificati e del protocollo TLS

Sommario

[Introduzione](#)

[Panoramica](#)

[Errori certificato](#)

[Certificato upstream scaduto](#)

[Certificato upstream autofirmato](#)

[Certificato intermedio mancante](#)

[Nome soggetto mancante nel certificato upstream.](#)

[Nome comune mancante nel certificato upstream.](#)

[Certificato upstream non attendibile](#)

[Il nome host nel certificato è diverso da quello previsto](#)

[Certificato upstream revocato](#)

[Errori handshake TLS](#)

[Crittografia Upstream Non Supportata](#)

[Versione TLS upstream non corrispondente](#)

[Chiave DH a monte inferiore a 1024 bit](#)

[Soluzioni](#)

Introduzione

In questo documento vengono descritti gli errori più comuni relativi ai certificati e ai protocolli TLS nella ricerca attività dashboard ombrella.

Panoramica

Il traffico HTTP bloccato a causa di errori di certificato e TLS ora può essere visualizzato nella ricerca attività dashboard ombrello. In questo articolo viene fornito un elenco di messaggi di errore comuni e una breve spiegazione per ognuno di essi.

Errori certificato

Certificato upstream scaduto

Un certificato presentato dal sito Web è scaduto. Per segnalare il problema, contattare il webmaster del sito.

Certificato upstream autofirmato

Il certificato del server presentato dal sito Web non è firmato da un'autorità di certificazione e pertanto Umbrella non è in grado di stabilire se il certificato è attendibile.

I certificati autofirmati vengono talvolta utilizzati quando un server ospita una risorsa destinata a un gruppo di destinatari con restrizioni. Ad esempio, i portali Web per le appliance di sicurezza IT spesso utilizzano certificati autofirmati. Impossibile configurare Umbrella per considerare attendibili i certificati autofirmati.

Certificato intermedio mancante

Umbrella non è stata in grado di ottenere certificati per tutte le autorità intermedie e quindi di convalidare l'intera catena di fiducia.

I certificati server Web vengono in genere rilasciati/firmati da un certificato intermedio di un'Autorità di certificazione. Tali certificati intermedi possono essere rilasciati anche da altri certificati intermedi. Il certificato del server Web (noto anche come "certificato foglia") e gli eventuali certificati intermedi formano una catena che riporta a un certificato radice. Affinché Umbrella possa convalidare l'intera catena di attendibilità, il sito Web deve includere i certificati intermedi nel certificato del server. Per segnalare il problema, contattare il webmaster del sito.

In alternativa, se il certificato include l'estensione "Accesso alle informazioni dell'autorità", Umbrella tenta di recuperare automaticamente le CA intermedie. Si noti che Umbrella supporta l'estensione AIA solo quando la decrittografia HTTPS e l'ispezione dei file sono abilitate.

Nome soggetto mancante nel certificato upstream.

Il campo Oggetto del certificato non contiene un nome distinto (DN) per identificare il certificato. Questo è un requisito per tutti i certificati rilasciati da un'Autorità di certificazione, e quindi richiesti da Cisco Umbrella. Per segnalare il problema, contattare il webmaster del sito.

Nome comune mancante nel certificato upstream.

Il certificato presentato dal sito Web non ha un nome comune. Il campo Nome comune (CN) è obbligatorio per Umbrella SWG. Contiene il nome host del certificato, necessario per verificare che il certificato corrisponda alla risorsa richiesta dall'utente (ad esempio, l'indirizzo digitato nel browser). Per segnalare il problema, contattare il webmaster del sito.

Certificato upstream non attendibile

Certificato non attendibile per Cisco Umbrella. Questo errore in genere indica che Cisco non considera attendibile la CA radice che ha emesso il certificato.

Umbrella SWG ha un elenco integrato di Autorità di certificazione radice note che aggiorniamo da una fonte attendibile. Se il certificato dei siti Web non è firmato da una CA dell'elenco, la convalida del certificato non riesce. Se si ritiene che a Umbrella manchi una CA radice affidabile, contattare il supporto tecnico.

Il nome host nel certificato è diverso da quello previsto

Risorsa richiesta dall'utente (ad esempio l'indirizzo digitato nel browser non corrisponde al nome comune (CN) o al nome alternativo del soggetto (SAN) del certificato, pertanto Umbrella non può considerare attendibile il certificato per questa richiesta. Per segnalare il problema, contattare il webmaster del sito.

Certificato upstream revocato

Il certificato fornito dal sito Web è stato revocato dall'autorità di certificazione che lo ha rilasciato.

Umbrella esegue controlli OCSP (Online Certificate Status Protocol) per determinare se un certificato è stato successivamente revocato da una CA. Per segnalare il problema, contattare il webmaster del sito.

Errori handshake TLS

Crittografia Upstream Non Supportata

Impossibile completare l'handshake TLS. Ciò significa che il sito Web non supporta nessuno degli elenchi di suite di cifratura utilizzati da Umbrella SWG. Questo errore può verificarsi con i server Web obsoleti o meno recenti che supportano solo le cifrature TLS più deboli. Per segnalare il problema, contattare il webmaster del sito.

Versione TLS upstream non corrispondente

Impossibile completare l'handshake TLS. Il sito Web non supporta la stessa versione TLS utilizzata da Umbrella SWG. Al momento, Umbrella SWG Proxy supporta TLS 1.2 e TLS 1.3 sia sulle connessioni lato client a Umbrella SWG che sulle connessioni proxy Umbrella SWG ai server Web di destinazione.

Chiave DH a monte inferiore a 1024 bit

Impossibile completare l'handshake TLS. Il sito Web utilizza una chiave Diffie-Hellman debole non supportata da Umbrella. Per segnalare il problema, contattare il webmaster del sito.

Soluzioni

È possibile risolvere questi problemi apportando modifiche alla configurazione in Cisco Umbrella. Questa operazione deve essere eseguita solo se si considera attendibile l'autenticità del server e del certificato.

Le soluzioni possono essere applicate usando una voce "Elenco di decrittografia selettiva" per disabilitare la decrittografia o una voce "Domini esterni" per ignorare completamente il traffico proveniente da Umbrella. Umbrella non esegue la convalida del certificato quando la decrittografia è disabilitata. Tenere presente che nella maggior parte dei casi il browser visualizza ancora un

errore o un avviso quando il traffico viene ignorato da Umbrella - i browser Web eseguono una convalida dei certificati simile.

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).