Errore di convalida del certificato di accesso sicuro con caricamenti del log del client di splunk

Sommario

Problema

I client Windows che eseguono il client Splunk non sono in grado di caricare i log nel cloud Splunk a causa di errori di convalida del certificato quando il traffico è stato decrittografato da Cisco Secure Access. Più di 5000 origini del registro di Windows non sono state in grado di inviare dati al cloud Splunk, con impatto sull'acquisizione del registro. L'errore specifico osservato nei log del client Splunk è:

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

Il traffico verso la destinazione *.splunkcloud.com scorreva attraverso il firewall, ma la convalida del certificato a livello di applicazione non è riuscita. L'esplorazione Web dei siti in cui è stata abilitata la decrittografia SSL ha continuato a funzionare normalmente.

Ambiente

- Cisco Secure Access con decrittografia SSL/TLS abilitata
- Client Windows con Splunk Universal Forwarder installato
- Destinazione cloud splunk: *.splunkcloud.com
- Più di 5.000 origini registro di Windows interessate
- Il client Splunk utilizza il proprio archivio certificati, non l'archivio certificati di sistema Microsoft

Risoluzione

Il problema è stato risolto implementando un criterio di bypass di decrittografia per il traffico Splunk cloud in Cisco Secure Access.

Sono state adottate diverse misure.

Passaggio 1: Identificazione del problema

Durante una sessione WebEx, il comportamento è stato confermato e riprodotto. I test hanno mostrato che quando la decrittografia Secure Access è stata disabilitata per un client o quando il servizio SWG è stato disabilitato sul client, il caricamento del log Splunk è riuscito. Ciò ha confermato che il processo di decrittografia SSL/TLS stava causando l'errore di convalida del certificato.

Passaggio 2: Crea elenco di destinazione

È stato creato un elenco di destinazione contenente gli FQDN e gli indirizzi IP del cloud Splunk per indirizzare in modo specifico il traffico destinato ai servizi cloud Splunk.

Passaggio 3: Implementa criterio di bypass decrittografia

È stato implementato un criterio Cisco Secure Access per disabilitare la decrittografia SSL/TLS per il traffico corrispondente all'elenco di destinazione Splunk Cloud. Questo criterio di bypass ha consentito ai client Splunk di stabilire connessioni crittografate dirette al cloud Splunk senza intercettazione dei certificati da parte di Secure Access.

Passaggio 4: Convalida

Dopo aver implementato il criterio di bypass della decrittografia, la convalida ha confermato che:

- I client di splunk sono stati in grado di caricare i log
- Il numero complessivo di client di reporting in Splunk cloud è aumentato notevolmente
- Non sono stati rilevati ulteriori errori di convalida del certificato

Il livello di gravità della richiesta è stato ridotto da 1 a 3 ed è stato posto in stato di monitoraggio per osservare il continuo e corretto caricamento del log.

Causa

La causa principale è che il client Splunk utilizza il proprio archivio certificati e non considera attendibile il certificato della CA secondaria primaria Cisco Secure Access presentato durante la decrittografia SSL/TLS. Quando Cisco Secure Access ha intercettato e decrittografato il traffico SSL verso Splunk cloud, lo ha crittografato di nuovo utilizzando la propria autorità di certificazione. Il processo di convalida del certificato del client Splunk ha rifiutato il certificato perché non è stato possibile verificare la catena di certificati restituendola a un'autorità di certificazione radice attendibile nel proprio archivio certificati.

L'errore di convalida X.509 specifico "impossibile ottenere il certificato dell'autorità emittente locale" (codice di errore 20) indica che il processo di convalida del certificato non è stato in grado di individuare l'autorità di certificazione emittente nell'archivio certificati attendibili del client, determinando l'esito negativo della connessione.

Contenuto correlato

- 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).