Errore di aggiornamento WSA da SMA a causa di una configurazione SSL non valida

Sommario

Problema

Quando si tenta di aggiornare un WSA (Web Security Appliance) da SMA (Security Management Appliance), il processo di aggiornamento non riesce e viene visualizzato il messaggio di errore "Aggiornamento non riuscito (motivo: configurazione SSL non valida)." L'aggiornamento è riuscito se eseguito direttamente dall'interfaccia Web WSA, ma ha sempre esito negativo se avviato dall'SMA. Tentativi non riusciti di risolvere il problema generando un nuovo certificato autofirmato e modificando il certificato di autenticazione predefinito.

Ambiente

- Cisco Web Security Appliance (WSA)
- Versione del software: 15.2.2-009 (MD)
- Cisco Security Management Appliance (SMA)
- Versione aggiornamento destinazione: AsyncOS 15.5
- Funzionalità DNS verificata e funzionante correttamente

Risoluzione

La risoluzione prevede la disabilitazione delle versioni TLS legacy (TLSv1.0 e TLSv1.1) sull'appliance WSA per soddisfare i prerequisiti di aggiornamento di AsyncOS 15.5.

Passaggio 1: Identificazione della root cause

L'errore di aggiornamento è causato da una modifica nel comportamento di AsyncOS 15.5 in cui TLSv1.0 e TLSv1.1 non sono più supportati in alcuna configurazione SSL diversa dalla configurazione proxy. Il processo di aggiornamento richiede TLSv1.2 o versioni successive per le configurazioni SSL non proxy.

Passaggio 2: Disabilita versioni TLS legacy

Disabilitare TLSv1.0 e TLSv1.1 sull'appliance WSA tramite l'interfaccia di configurazione. Questa modifica soddisfa il prerequisito per l'aggiornamento e consente di continuare il processo di aggiornamento.

Passaggio 3: Verifica compatibilità servizio esterno

Garantire il supporto di servizi esterni, quali LDAP, TLSv1.2 o versioni successive. Finché questi servizi sono compatibili con TLSv1.2 e versioni successive, l'aggiornamento non interrompe la comunicazione con i sistemi esterni.

Passaggio 4: Continua l'aggiornamento

Dopo aver disattivato le versioni TLS legacy, riprovare il processo di aggiornamento da SMA. L'aggiornamento può ora procedere senza l'errore "Configurazione SSL non valida".

Passaggio 5: Monitoraggio e convalida

Monitorare il processo di aggiornamento per garantirne il corretto completamento e verificare che tutti i servizi dipendenti continuino a funzionare correttamente con TLSv1.2 dopo l'aggiornamento.

Causa

L'errore di aggiornamento è causato da una modifica del comportamento introdotta in AsyncOS 15.5.0-566, dove TLSv1.0 e TLSv1.1 non sono più supportati in alcuna configurazione SSL diversa dalla configurazione proxy. In questo modo viene creato un prerequisito di aggiornamento che richiede la modifica della versione TLS in TLSv1.2 o versioni successive prima dell'aggiornamento di AsyncOS. Il processo di aggiornamento di SMA esegue controlli di convalida pre-aggiornamento che rilevano questa incompatibilità e impediscono il proseguimento dell'aggiornamento.

Contenuto correlato

- Note sulla release di AsyncOS 15.5
- 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).