Error de actualización de WSA desde SMA debido a una configuración SSL no válida

Contenido

Problema

Al intentar actualizar un WSA (dispositivo de seguridad web) desde SMA (dispositivo de administración de seguridad), el proceso de actualización falla con el mensaje de error "Error al actualizar al actualizar (motivo: Configuración SSL no válida)." La actualización se realiza correctamente cuando se realiza directamente desde la interfaz web de WSA, pero siempre falla cuando se inicia desde el SMA. Los intentos de resolver el problema generando un nuevo certificado autofirmado y cambiando el certificado de autenticación predeterminado no se realizaron correctamente.

Entorno

- Dispositivo de seguridad Cisco Web Security Appliance (WSA)
- Versión del software: 15.2.2-009 (MD)
- Dispositivo de administración de seguridad de Cisco (SMA)
- Versión de actualización de destino: AsyncOS 15.5
- Funcionalidad de DNS verificada y que funciona correctamente

Resolución

La resolución implica deshabilitar las versiones de TLS antiguas (TLSv1.0 y TLSv1.1) en el dispositivo WSA para cumplir los requisitos previos de actualización para AsyncOS 15.5.

Paso 1: Identificar la causa raíz

La falla de actualización es causada por un cambio en el comportamiento de AsyncOS 15.5 donde TLSv1.0 y TLSv1.1 ya no se soportan en ninguna configuración SSL que no sea la configuración de proxy. El proceso de actualización requiere TLSv1.2 o posterior para las configuraciones SSL no proxy.

Paso 2: Deshabilitar versiones antiguas de TLS

Desactive TLSv1.0 y TLSv1.1 en el dispositivo WSA a través de la interfaz de configuración. Este cambio satisface el requisito previo de actualización y permite que el proceso de actualización continúe.

Paso 3: Verificar la compatibilidad del servicio externo

Asegúrese de que los servicios externos como LDAP admitan TLSv1.2 o versiones posteriores. Mientras estos servicios sean compatibles con TLSv1.2 y versiones posteriores, la actualización no interrumpe la comunicación con los sistemas externos.

Paso 4: Continuar con la actualización

Después de deshabilitar las versiones de TLS heredadas, vuelva a intentar el proceso de actualización desde el SMA. La actualización ahora puede continuar sin el error "Invalid SSL configuration".

Paso 5: Supervisión y validación

Supervise el proceso de actualización para asegurarse de que la finalización y validación de todos los servicios dependientes continúa funcionando correctamente con TLSv1.2 después de la actualización.

Causa

La falla de actualización es causada por un cambio de comportamiento introducido en AsyncOS 15.5.0-566 donde TLSv1.0 y TLSv1.1 ya no se soportan en ninguna configuración SSL que no sea la configuración proxy. Esto crea un requisito previo de actualización que requiere cambiar la versión de TLS a TLSv1.2 o posterior antes de actualizar AsyncOS. El proceso de actualización de SMA realiza comprobaciones de validación previas a la actualización que detectan esta incompatibilidad y evitan que la actualización continúe.

Contenido relacionado

- Notas de la versión de AsyncOS 15.5
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).