Falha na atualização do WSA do SMA devido à configuração de SSL inválida

Contents

Problema

Ao tentar atualizar um WSA (Web Security Appliance) do SMA (Security Management Appliance), o processo de atualização falha com a mensagem de erro "Falha ao atualizar atualização (Motivo: configuração de SSL inválida)." A atualização é bem-sucedida quando executada diretamente na interface da Web do WSA, mas falha de forma consistente quando iniciada no SMA. As tentativas de resolver o problema gerando um novo certificado autoassinado e alterando o certificado de autenticação padrão não tiveram êxito.

Ambiente

- Cisco Web Security Appliance (WSA)
- Versão de software: 15.2.2-009 (MD)
- Cisco Security Management Appliance (SMA)
- Versão de Atualização de Destino: AsyncOS 15.5
- Funcionalidade DNS verificada e funcionando corretamente

Resolução

A resolução envolve desabilitar versões TLS herdadas (TLSv1.0 e TLSv1.1) no dispositivo WSA para atender aos pré-requisitos de atualização para AsyncOS 15.5.

Passo 1: Identificar a causa raiz

A falha de atualização é causada por uma alteração no comportamento do AsyncOS 15.5, em que TLSv1.0 e TLSv1.1 não são mais suportados em qualquer configuração SSL diferente da configuração de proxy. O processo de atualização requer TLSv1.2 ou posterior para configurações SSL não proxy.

Passo 2: Desabilitar versões TLS antigas

Desabilite o TLSv1.0 e o TLSv1.1 no dispositivo WSA por meio da interface de configuração. Essa alteração satisfaz o pré-requisito de atualização e permite que o processo de atualização continue.

Passo 3: Verificar Compatibilidade de Serviço Externo

Garantir serviços externos, como suporte LDAP para TLSv1.2 ou versões posteriores. Desde que esses serviços sejam compatíveis com TLSv1.2 e posterior, a atualização não interrompe a comunicação com sistemas externos.

Passo 4: Prosseguir com a atualização

Depois de desabilitar as versões TLS herdadas, repita o processo de atualização do SMA. A atualização agora pode continuar sem o erro "Configuração de SSL inválida".

Passo 5: Monitorar e validar

Monitore o processo de atualização para garantir a conclusão bem-sucedida e valide se todos os serviços dependentes continuam a funcionar corretamente com TLSv1.2 após a atualização.

Causa

A falha de atualização é causada por uma alteração comportamental introduzida no AsyncOS 15.5.0-566, onde TLSv1.0 e TLSv1.1 não são mais suportados em qualquer configuração SSL diferente da configuração proxy. Isso cria um pré-requisito de atualização que requer a alteração da versão do TLS para TLSv1.2 ou posterior antes da atualização do AsyncOS. O processo de atualização do SMA executa verificações de validação pré-atualização que detectam essa incompatibilidade e impedem que a atualização prossiga.

Conteúdo relacionado

- Notas da versão do AsyncOS 15.5
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.