Fout bij WSA-upgrade van SMA vanwege ongeldige SSL-configuratie

Inhoud

uitgifte

Wanneer u probeert een WSA (Web Security Appliance) te upgraden van SMA (Security Management Appliance), mislukt het upgradeproces met de foutmelding "Update mislukt om te upgraden (Reden: Ongeldige SSL-configuratie)." De upgrade is succesvol wanneer deze rechtstreeks vanuit de WSA-webinterface wordt uitgevoerd, maar mislukt consistent wanneer deze vanuit de SMA wordt geïnitieerd. Pogingen om het probleem op te lossen door een nieuw zelfondertekend certificaat te genereren en het standaardverificatiecertificaat te wijzigen, zijn mislukt.

milieu

- Cisco Web Security Appliance (WSA)
- Softwareversie: 15.2.2-009 (MD)
- Cisco Security Management Appliance (SMA)
- Doelversie van de upgrade: AsyncOS 15.5
- DNS-functionaliteit geverifieerd en correct werkt

resolutie

De resolutie omvat het uitschakelen van oudere TLS-versies (TLSv1.0 en TLSv1.1) op het WSA-toestel om te voldoen aan de upgradevereisten voor AsyncOS 15.5.

Stap 1: Identificeer de oorzaak

De upgradefout wordt veroorzaakt door een wijziging in het gedrag van AsyncOS 15.5 waarbij TLSv1.0 en TLSv1.1 niet langer worden ondersteund in een andere SSL-configuratie dan de proxyconfiguratie. Voor het upgradeproces is TLSv1.2 of hoger vereist voor SSL-configuraties zonder proxy.

Stap 2: Legacy TLS-versies uitschakelen

Schakel TLSv1.0 en TLSv1.1 uit op het WSA-toestel via de configuratie-interface. Deze wijziging voldoet aan de upgradevoorwaarde en zorgt ervoor dat het upgradeproces kan worden voortgezet.

Stap 3: Verifieer de compatibiliteit van externe services

Zorg voor externe services zoals LDAP-ondersteuning voor TLSv1.2 of latere versies. Zolang deze services compatibel zijn met TLSv1.2 en hoger, verbreekt de upgrade de communicatie met externe systemen niet.

Stap 4: Doorgaan met upgraden

Nadat u de oudere TLS-versies hebt uitgeschakeld, probeert u het upgradeproces opnieuw vanuit de SMA. De upgrade kan nu worden uitgevoerd zonder de fout "Ongeldige SSL-configuratie".

Stap 5: controleren en valideren

Controleer het upgradeproces om ervoor te zorgen dat alle afhankelijke services met TLSv1.2 na de upgrade goed blijven functioneren.

Oorzaak

De upgrade-fout wordt veroorzaakt door een gedragswijziging die is geïntroduceerd in AsyncOS 15.5.0-566, waarbij TLSv1.0 en TLSv1.1 niet langer worden ondersteund in een andere SSL-configuratie dan de proxyconfiguratie. Dit creëert een upgradevereiste die vereist dat de TLS-versie wordt gewijzigd in TLSv1.2 of hoger voordat AsyncOS wordt geüpgraded. Het SMA-upgradeproces voert validatiecontroles vóór de upgrade uit om deze incompatibiliteit te detecteren en te voorkomen dat de upgrade wordt uitgevoerd.

Gerelateerde inhoud

- AsyncOS 15.5 Release-opmerkingen
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.