Warnungen zum Ablauf des SSE Connector-Zertifikats und automatischer Verlängerungsprozess

Inhalt

Problem

Benutzer erhalten in ihren täglichen Wartungsberichten für Cisco SSE (Secure Service Edge) Ablaufwarnungen für Zertifikate, die darauf hinweisen, dass Connector-Zertifikate innerhalb von 30 Tagen ablaufen. Der Wartungsbericht zeigt Warnungen wie "Cert Expiry Warning (<=30 days)" (Warnung vor Ablauf des Zertifikats (<=30 Tage))" für angeschlossene SSE-Konnektoren an und gibt Anlass zur Sorge, ob Maßnahmen zur Aufrechterhaltung der Konnektivität und des sicheren Zugriffs erforderlich sind.

Die jeweilige Warnung wird im Format des Berichts für die tägliche Wartung angezeigt:

```
*** CISCO SSE DAILY MAINTENANCE REPORT ***
Report Time : 2026-05-12T12:18:07Z
Total : 2 connector(s)

SUMMARY
------------------------------------------------
- Cert Expiry Critical (<=7 days) : 0
- Cert Expiry Warning (<=30 days) : 2
- Vulnerable (CVE) : 0
- Upgrade Failed : 0
- Outdated Base Version : 0
- Stale Status (>24h no update) : 0

========================================
WARNING -- CERTIFICATES EXPIRING WITHIN 30 DAYS
========================================
------------------------------------------------
- Hostname : <>
- ID : <>
- Status : connected
- Cert Expires : 2026-06-02T00:13:52Z
- Version : v2.0.94
------------------------------------------------
- Hostname : <>
- ID : <>
- Status : connected
```

```
- Cert Expires : 2026-05-28T23:12:35Z
```

Umwelt

- Cisco Secure Access (SSE)-Plattform mit bereitgestellten Remote Connectors
- SSE-Connectors zeigen in Wartungsberichten den Status "verbunden" an
- Connector-Versionen einschließlich v2.0.94 und ähnliche Versionen
- Tägliche Wartungsberichte für die Zertifikatsüberwachung aktiviert

Auflösung

Die Ablaufwarnungen für Zertifikate in den täglichen Wartungsberichten von SSE sind normal und erfordern von Ihrer Seite keine Maßnahmen. Die Zertifikatverlängerung wird von der SSE-Plattform automatisch über diesen Prozess durchgeführt.

Verhalten bei der Zertifikatverlängerung

Cisco SSE Connector-Zertifikate werden automatisch und ohne Ihren Eingriff erneuert. Die Warnmeldungen dienen als informative Warnmeldungen zu bevorstehenden Verlängerungsaktivitäten und nicht als Aktionspunkte, für die eine manuelle Zertifikatverwaltung erforderlich ist.

Erforderliche Bedingungen für die automatische Verlängerung

Um eine erfolgreiche automatische Zertifikatverlängerung sicherzustellen, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

Schritt 1: Status des Remote-Anschlusses überprüfen

Stellen Sie sicher, dass der Remote Connector (RC) ausgeführt wird und während der Erneuerung des Zertifikats nicht heruntergefahren wird. Der Steckverbinder muss in betriebsbereitem Zustand bleiben, um die automatische Verlängerung abzuschließen.

Phase 2: Netzwerkverbindungen überprüfen

Vergewissern Sie sich, dass die Remote Connector-Kommunikation mit Cisco SSE-Services nicht durch Firewall-Regeln blockiert wird. Der RC erfordert ausgehende Verbindungen, um Vorgänge zur Erneuerung des Zertifikats abzuschließen.

Überwachung und Validierung

Nach Ablauf des Zertifikats werden in den täglichen Wartungsberichten keine Warnungen mehr zum Ablauf des Zertifikats für die erneuerten Zertifikate angezeigt. Der Status des Connectors muss während des gesamten Verlängerungsprozesses "Connected" bleiben.

Wenn nach der Erneuerung des Zertifikats eine zusätzliche Validierung erforderlich ist, z. B. das Überprüfen von Verlängerungsereignissen in Protokollen oder das Bestätigen der Konnektivität nach der Verlängerung, kann eine detaillierte Protokollanalyse durchgeführt werden, um den Abschluss der Verlängerung zu validieren.

Ursache

Die Zertifikatsablaufwarnungen werden vom proaktiven Überwachungssystem der SSE-Plattform generiert, das Benutzer innerhalb eines Zeitfensters von 30 Tagen über Zertifikate informiert, die ihr Ablaufdatum erreichen. Dieses Verhalten soll Transparenz für das Zertifikat-Lebenszyklus-Management bieten, auch wenn der Verlängerungsprozess automatisiert ist.

Verwandte Inhalte

- Cisco Secure Access-Dokumentation

- Cisco Secure Access Remote Connector - Dokumentation
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.