Fehler bei der Validierung des Zertifikats für sicheren Zugriff durch Uploads von Splunk-Clientprotokollen

Inhalt

Problem

Windows-Clients, auf denen der Splunk-Client ausgeführt wird, konnten aufgrund von Zertifikatsüberprüfungsfehlern beim Entschlüsseln des Datenverkehrs durch Cisco Secure Access keine Protokolle in die Splunk-Cloud hochladen. Mehr als 5.000 Windows-Protokollquellen konnten keine Daten an die Splunk-Cloud senden, was sich auf die Protokollaufnahme auswirkt. Der in den Splunk-Client-Protokollen festgestellte spezifische Fehler war:

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

Der Datenverkehr zum Ziel *.splunkcloud.com wurde über die Firewall weitergeleitet, die Validierung des Zertifikats auf Anwendungsebene schlug jedoch fehl. Das Surfen im Internet auf Websites, auf denen die SSL-Entschlüsselung aktiviert war, funktionierte weiterhin normal.

Umwelt

- Cisco Secure Access mit aktivierter SSL/TLS-Verschlüsselung
- Windows-Clients mit installiertem Splunk Universal Forwarder
- Splunk-Cloud-Ziel: * .splunkcloud.com
- Mehr als 5000 Windows-Protokollquellen betroffen
- Der Splunk-Client verwendet seinen eigenen Zertifikatspeicher, nicht den Microsoft-Systemzertifikatsspeicher.

Auflösung

Das Problem wurde durch die Implementierung einer Richtlinie zur Umgehung der Entschlüsselung für Splunk-Cloud-Datenverkehr in Cisco Secure Access behoben.

Es wurden mehrere Schritte unternommen.

Schritt 1: Identifizieren des Problems

Während einer WebEx Sitzung wurde das Verhalten bestätigt und reproduziert. Die Tests haben gezeigt, dass das Hochladen von Splunk-Protokollen erfolgreich war, wenn die Entschlüsselung von Secure Access für einen Client oder der SWG-Dienst auf dem Client deaktiviert wurde. Dadurch wurde bestätigt, dass der SSL/TLS-Entschlüsselungsprozess den Fehler bei der Zertifikatsvalidierung verursacht hat.

Phase 2: Zielliste erstellen

Es wurde eine Zielliste erstellt, die die Splunk-Cloud-FQDNs und IP-Adressen enthält, um Datenverkehr, der für Splunk-Cloud-Services bestimmt ist, gezielt anzusprechen.

Schritt 3: Implementierung einer Richtlinie zur Umgehung der Entschlüsselung

Eine Cisco Secure Access-Richtlinie wurde implementiert, um die SSL/TLS-Entschlüsselung für Datenverkehr zu deaktivieren, der mit der Splunk-Cloud-Zielliste übereinstimmt. Diese Umgehungsrichtlinie ermöglichte es Splunk-Clients, direkt verschlüsselte Verbindungen zur Splunk-Cloud herzustellen, ohne dass ein Zertifikatabbruch durch Secure Access erforderlich war.

Schritt 4: Validierung

Nach der Implementierung der Richtlinie zur Umgehung der Entschlüsselung hat die Validierung Folgendes bestätigt:

- Splunk-Clients konnten Protokolle erfolgreich hochladen
- Die Gesamtzahl der Reporting-Clients in der Splunk-Cloud hat sich deutlich erhöht.
- Es wurden keine weiteren Zertifikatvalidierungsfehler festgestellt

Der Schweregrad des Falls wurde von 1 auf 3 reduziert und in den Überwachungsstatus versetzt, um die weitere erfolgreiche Protokollierung zu beobachten.

Ursache

Die Ursache war, dass der Splunk-Client seinen eigenen Zertifikatspeicher verwendet und dem primären SubCA-Zertifikat von Cisco Secure Access, das während der SSL/TLS-Entschlüsselung vorgelegt wurde, nicht vertraut. Beim Abfangen und Entschlüsseln des SSL-Datenverkehrs zur Splunk-Cloud durch Cisco Secure Access wurde der Datenverkehr mithilfe der eigenen Zertifizierungsstelle erneut verschlüsselt. Der Validierungsprozess des Splunk-Clientzertifikats hat dieses Zertifikat zurückgewiesen, da es die Zertifikatkette nicht an eine vertrauenswürdige Stammzertifizierungsstelle in ihrem eigenen Zertifikatspeicher zurücküberprüfen konnte.

Der spezifische X.509-Validierungsfehler "kann kein lokales Ausstellerzertifikat abrufen" (Fehlercode 20) gibt an, dass der Zertifikatvalidierungsprozess die ausstellende Zertifizierungsstelle nicht im vertrauenswürdigen Zertifikatspeicher des Clients finden konnte, wodurch die Verbindung fehlschlug.

Verwandte Inhalte

- 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.