Beheben Sie den durch den Quiet-Modus für Anmeldungsblöcke verursachten intermittierenden SSH-Zugriffsfehler auf IOS XE-Geräten.

Inhalt

Problem

Geräte mit IOS XE-Software weisen zeitweilig SSH-Zugriffsfehler auf. SSH-Verbindungen werden manchmal akzeptiert und manchmal ohne konsistentes Muster abgelehnt. Der Konsolenzugriff auf die Geräte ist nicht betroffen. Bei einer fehlgeschlagenen SSH-Sitzung bestätigen die auf dem betroffenen Gerät durchgeführten Paketerfassungen, dass das Gerät selbst TCP-RST-Pakete direkt nach Empfang der TCP-SYN des Clients gesendet hat, bevor die SSH-Sitzung überhaupt mit der Aushandlung beginnen konnte. Wenn der Befehl debug ip tcp transactions enabled ist, veranschaulicht die folgende Debug-Ausgabe das TCP-RST-Verhalten:

```
Aug 21 19:46:04.697: Reserved port 0 in Transport Port Agent for TCP IP type 0
Aug 21 19:46:04.697: TCP: sending RST, seq 0, ack 1013312911
Aug 21 19:46:04.697: TCP: sent RST to 10.x.x.x:43266 from 10.x.x.x:22
Aug 21 19:46:04.698: Released port 0 in Transport Port Agent for TCP IP type 0 delay 0
Aug 21 19:46:04.698: TCP0: state was LISTEN -> CLOSED [0 -> UNKNOWN(0)]
Aug 21 19:46:04.698: TCB destroyed
```

Überprüfen Sie die folgenden Elemente, um sie als beitragende Ursachen auszuschließen:

- Verwenden Sie den Befehl show ip ssh, um zu bestätigen, dass SSH auf dem Gerät aktiviert ist.
- Verwenden Sie den Befehl show tcp brief, um zu bestätigen, dass der TCP-Port 22 innerhalb des IOSd-Prozesses überwacht wird.
- In der Ausgabe des Befehls show ip traffic or debug ip error gibt es keinen "no port"-Fehler
- VTY-Leitungen sind nicht vollständig belegt; In der Befehlsausgabe von show line werden nicht alle Leitungen belegt angezeigt.

- Das Problem besteht auch nach dem Entfernen der Access-Class-Konfiguration für die VTY-Leitungen weiter.

Der Geräteprotokollierungspuffer zeigte eine sehr große Anzahl wiederholter Authentifizierungsfehler sowie einen aktiven Ruhezustand an:

```
Aug 21 12:24:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: test_user] [Source: LOCAL] [localport: 
Aug 21 12:24:32: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 0 secs, [user: tes
```

Die Ausgabe show login at the time of the failure zeigt an, dass sich das Gerät zum Zeitpunkt des SSH-Ausfalls im stillen Modus befindet.

Umwelt

- Plattform: Cisco Catalyst Switches der Serie 9500 (Core-Switch und Managed Switch-Stacks)
- SSH ist für den Remote-Zugriff auf das Gerät aktiviert.
- Auf dem Gerät aktivierte Konfiguration für die Blockierung der Anmeldung: Anmeldeblock - für 120 Versuche 3 innerhalb von 60

Auflösung

Dieses Problem wird dadurch verursacht, dass die Funktion Anmeldeblock im stillen Modus dauerhaft durch eine große Anzahl fehlgeschlagener Authentifizierungsversuche ausgelöst wird. Verwenden Sie zur Behebung des Problems eine Zugriffsklassenzugriffskontrollliste im stillen Modus für vertrauenswürdige SSH-Verwaltungsgeräte.

Konfigurieren des Anmeldeblocks mit einer vertrauenswürdigen Zugriffskontrollliste der Quiet-Mode-Klasse

Konfigurieren Sie die Anmeldeblockfunktion, und implementieren Sie eine Zugriffskontrollliste (Access Control List, ACL) für den stillen Modus. Diese ACL ermöglicht vertrauenswürdigen Management-Hosts und Subnetzen, die Durchsetzung des stillen Modus zu umgehen, während der Schutz des Anmeldeblocks für alle anderen Quellen aktiv bleibt.

1. Definieren Sie eine benannte erweiterte ACL, die die vertrauenswürdigen Management-Hosts und -Subnetze zulässt. Im folgenden Beispiel sind zwei spezifische Jump-Host-IPs und ein /22-Management-Subnetz zulässig. Passen Sie die Einträge an die vertrauenswürdigen Managementquellen in der Umgebung an:

```
device# configure terminal
device(config)# ip access-list extended quietmode_trusted_ip
device(config-ext-nacl)# 10 permit ip host <trusted_host_1_ip> any
device(config-ext-nacl)# 20 permit ip host <trusted_host_2_ip> any
device(config-ext-nacl)# 30 permit ip <subnet_address> <wildcard_mask> any
device(config-ext-nacl)# exit
```

Für den Aufbau eines ACL-Eintrags:

- Verwenden Sie das host-Schlüsselwort gefolgt von einer einzelnen IP-Adresse, um einen bestimmten Management-Host (z. B. einen Jump-Server) zuzulassen.
- Um ein ganzes Subnetz zuzulassen, geben Sie die Netzwerkadresse gefolgt von der entsprechenden Platzhaltermaske ein.

2. Wenden Sie die ACL auf die Zugriffsklasse im stillen Modus an, damit Quellen, die mit der ACL übereinstimmen, eine Verbindung herstellen können, auch wenn der stille Modus aktiv ist:

```
device(config)# login quiet-mode access-class quietmode_trusted_ip
device(config)# end
```

3. Aktivieren Sie den Konfigurationsbefehl login block-for erneut, wenn er entfernt wurde:

```
device# configure terminal
device(config)# login block-for 120 attempts 3 within 60
device(config)# end
```

4. Konfiguration speichern:

```
device# write memory
```

5. Überwachen Sie das Systemprotokoll, um festzustellen, ob der stille Modus weiterhin ausgelöst wird, und den aktuellen Anmeldemodus:

```
device# show logging
device# show login
```

Beheben der dauerhaften Authentifizierungsfehler-Ursache

Die oben beschriebene, auf ACL basierende Problemumgehung behebt das Symptom (SSH wird im stillen Modus blockiert), geht jedoch nicht auf die zugrunde liegende Ursache ein, d. h. die große Anzahl wiederholter Authentifizierungsfehler. Diese Ausfälle lösen kontinuierlich den Ruhezustand aus. Um das Problem vollständig zu beheben, sollte das häufige Authentifizierungsproblem untersucht und behoben werden.

Ursache

Die zeitweiligen SSH-Zugriffsfehler werden dadurch verursacht, dass die IOS-XE-Anmeldeblockierfunktion in den stillen Modus wechselt, da viele Authentifizierungsversuche fehlgeschlagen sind. Beispiel für einen Anmeldeblock zur Konfiguration:

```
login block-for 120 attempts 3 within 60
```

Mit dieser Konfiguration wird das IOS XE-Gerät angewiesen, in den stillen Modus zu wechseln und alle neuen Anmeldeverbindungen für 120 Sekunden zu blockieren, wenn innerhalb eines 60-Sekunden-Fensters drei oder mehr fehlgeschlagene Anmeldeversuche erkannt werden. Eine große Anzahl fehlgeschlagener Authentifizierungsversuche löst ständig den stillen Anmeldemodus aus. Die Durchsetzung des Quiet-Modus ist global und gilt für alle VTY-Leitungen und alle für SSH konfigurierten TCP-Ports. Wenn der stille Modus aktiv ist, sendet das Gerät sofort nach Empfang eines neuen TCP-SYN-Pakets von einer Quelle, die nicht explizit durch eine Zugriffskontrollliste für den stillen Modus zugelassen ist, ein TCP-RST-Paket, wodurch die Einrichtung der SSH-Sitzung verhindert wird.

Verwandte Inhalte

- Cisco IOS-XE Security Configuration Guide: Verbesserungen bei der Anmeldung (Anmelde-Zugangsklasse mit Block- und Quiet-Modus)
- 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.