

Ereignisse der VPN-Authentifizierung für sicheren Zugriff mit Link-Local-AAA-Serveradressen

Inhalt

Problem

Beim Testen der VPN-Funktion für sicheren Zugriff auf Remote-Zugriff (RA) werden übermäßige Authentifizierungsereignisse für Identitäten protokolliert, die in der Tenant-Organisation nicht vorhanden sind. Die Authentifizierungsprotokolle zeigen mehr als 10.000 RA VPN-Authentifizierungsereignisse innerhalb eines Zeitraums von 24 Stunden an, die AAA-Fehler wie "AAALOG_SERVICE_DOWN" und "AAALOG_SERVER_DOWN" enthalten. Diese Fehlermeldungen beziehen sich auf link-local 169.254.x.x-Adressen als AAA-Server, die nicht im Tenant konfiguriert sind.

Folgende Fehlerbeispiele wurden in den Protokollen beobachtet:

```
AAALOG_SERVICE_DOWN
AAA authentication server not accessible : server = 169.254.169.79 : user = <user>

AAALOG_SERVER_DOWN
AAA Marking RADIUS server 169.254.169.79 as FAILED
```

Bei den Aktivitäten handelt es sich anscheinend um wiederholte RADIUS-basierte Authentifizierungsversuche gegen den Secure Access VPN FQDN, die ein übermäßiges Protokollrauschen verursachen und Bedenken hinsichtlich externer Scans oder eines möglichen Missbrauchs des VPN-Dienstes aufwerfen.

Umwelt

- Cisco Secure Access-Plattform

- VPN-Profil für Remote-Zugriff, das ursprünglich ohne Zertifikatsauthentifizierung konfiguriert wurde
- Für RA VPN konfigurierte RADIUS-basierte Authentifizierung
- Öffentliche VPN-Tenant-Konfiguration mit erkennbaren VPN-Profilen

Auflösung

Die Lösung bestand darin, das Verhalten des Authentifizierungsflusses zu verstehen und eine zertifikatbasierte Authentifizierung als Strategie zur Risikominimierung zu implementieren.

Technische Erläuterung des beobachteten Verhaltens

Übermäßige Authentifizierungsereignisse treten aus den in den nächsten Abschnitten beschriebenen technischen Gründen auf.

Authentifizierungsablauf ohne Zertifikatanforderungen

Wenn die Zertifikatsauthentifizierung deaktiviert und die RADIUS-basierte RA VPN-Authentifizierung verwendet wird, protokolliert das System "fehlgeschlagene Autorisierungsversuche", da das System zunächst die Identität des Benutzernamens mit der Datenbank der in Secure Access synchronisierten Benutzer vergleicht und das Ereignis "fehlgeschlagene Autorisierung" aufzeichnet. Diese Ereignisse stellen eine erste Verteidigungslinie dar, können jedoch zu erheblichen Protokollfehlern führen, wenn externe Akteure versuchen, sich zu authentifizieren.

Link-Lokale Adressverwendung

Bei den 169.254.x.x-Adressen in den Protokollen handelt es sich um interne bzw. lokale Verbindungsadressen, die vom RA VPN-Headend zur Autorisierung eingehender Sitzungen verwendet werden. Diese Adressen repräsentieren das interne Systemverhalten anstelle einer falschen Konfiguration von AAA-Servern im Tenant.

VPN-Profilerkennung

Wenn eine öffentliche VPN-Tenant-ID konfiguriert wird, werden die VPN-Profile in der Dropdown-Liste "Benutzeroberfläche" aufgeführt, sodass externe Akteure öffentliche Profile leichter erkennen und für Authentifizierungsversuche gezielt einsetzen können.

Sofortige Eindämmungsschritte

1.- Konfigurieren Sie die zertifikatbasierte Authentifizierung. Ändern Sie das RA VPN-Profil so, dass eine zertifikatbasierte Authentifizierung erforderlich ist. Wenn eine Zertifikatsauthentifizierung erforderlich ist, führt Secure Access eine Zertifikatsüberprüfung zu einem früheren Zeitpunkt im Authentifizierungsablauf durch. Wenn das Zertifikat fehlt, erzeugt das System einen Fehler vor dem standardmäßigen Authentifizierungsablauf, und die Ereignisse bei der "fehlgeschlagenen Autorisierung" werden nicht auf die gleiche Weise protokolliert.

2.- Validierung der Effektivität der Risikominimierung Überwachen Sie die Authentifizierungsprotokolle nach der Implementierung der zertifikatbasierten Authentifizierung, um die Reduzierung übermäßiger Authentifizierungseignisse zu bestätigen. Der Wechsel zur zertifikatbasierten Authentifizierung hat die Angriffe erfolgreich eingedämmt und Protokollgeräusche reduziert.

Langfristige Verbesserungen

Es wurden zwei Funktionsanforderungen erstellt, um die zugrunde liegenden Probleme zu beheben:

- Feature-Anforderung 1: Fügen Sie beim Hinzufügen eines öffentlichen VPN-Tenants eine Option zum Ausblenden oder Anzeigen der Tunnelgruppenliste (VPN-Profil) hinzu, um die Profilermittlung zu reduzieren.
- Feature-Anforderung 2: Fügen Sie eine Konfigurationsoption hinzu, um die Protokollierung fehlgeschlagener RA VPN-Autorisierungsversuche zu aktivieren oder zu deaktivieren. So erhalten Administratoren die Kontrolle über den Ausführlichkeitsgrad des Protokolls.

Darüber hinaus wird ein öffentlich zugängliches Dokument erstellt, in dem die protokollierten Ereignisse und das Authentifizierungsverhalten erläutert werden, damit Administratoren den

normalen Systembetrieb besser verstehen können.

Ursache

Die Ursache für übermäßige Authentifizierungsereignisse liegt in der Kombination erkennbarer VPN-Profiles in Public-Tenant-Konfigurationen und dem Verhalten des Authentifizierungsflusses, wenn keine zertifikatbasierte Authentifizierung erforderlich ist. Wenn die RADIUS-basierte Authentifizierung ohne Zertifikatanforderungen verwendet wird, protokolliert das System alle "fehlgeschlagenen Autorisierungsversuche" als Teil seines Sicherheitsstatus, einschließlich der Versuche externer Akteure, die die VPN-Profile erkennen. Die Link-Local-Adressen in den Protokollen stellen das normale interne Systemverhalten für den RA VPN-Headend-Autorisierungsprozess dar, nicht Konfigurationsfehler.

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.