

Eventos de autenticación VPN de RA de acceso seguro con direcciones de servidor AAA locales de enlace

Contenido

Problema

Al probar la funcionalidad VPN de acceso remoto seguro (RA), se registran eventos de autenticación excesivos para las identidades que no existen en la organización de arrendatarios. Los registros de autenticación muestran más de 10.000 eventos de autenticación VPN de RA en un período de 24 horas, que contienen errores AAA como "AAALOG_SERVICE_DOWN" y "AAALOG_SERVER_DOWN". Estos mensajes de error hacen referencia a las direcciones locales de link 169.254.x.x como el servidor AAA, que no están configuradas en el arrendatario.

Entre los ejemplos de errores específicos observados en los registros se incluyen:

```
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
```

La actividad parece ser repetidos intentos de autenticación basados en RADIUS contra el FQDN de VPN de acceso seguro, lo que crea un ruido de registro excesivo y genera preocupación sobre el escaneo externo o el abuso potencial del servicio VPN.

Entorno

- Plataforma Cisco Secure Access
- Perfil VPN de acceso remoto configurado inicialmente sin autenticación de certificado

- Autenticación basada en RADIUS configurada para VPN de RA
- Configuración de arrendatario de VPN pública con perfiles de VPN detectables

Resolución

La resolución implicaba entender el comportamiento del flujo de autenticación e implementar la autenticación basada en certificados como una estrategia de mitigación.

Explicación técnica del comportamiento observado

Los eventos de autenticación excesivos ocurren debido a las razones técnicas descritas en las siguientes secciones.

Flujo de autenticación sin requisitos de certificado

Cuando la autenticación de certificados está deshabilitada y se utiliza la autenticación VPN de RA basada en RADIUS, el sistema registra los intentos de "autorización errónea" porque primero comprueba la identidad del nombre de usuario con la base de datos de usuarios sincronizados en Secure Access y registra el evento de "autorización errónea". Estos eventos se esperan como una primera línea de defensa, pero pueden producir un ruido de registro significativo cuando los actores externos intentan la autenticación.

Uso de la dirección local del enlace

Las direcciones 169.254.x.x que se ven en los registros son direcciones de link interno/local utilizadas por la cabecera VPN de RA para autorizar sesiones entrantes. Estas direcciones representan el comportamiento interno del sistema en lugar de la configuración incorrecta de los servidores AAA en el arrendatario.

Detección de perfiles VPN

Cuando se configura una ID de arrendatario de VPN pública, los perfiles de VPN se enumeran en el menú desplegable de la interfaz de usuario, lo que puede permitir que los actores externos descubran los perfiles públicos con mayor facilidad y los seleccionen para los intentos de autenticación.

Pasos inmediatos de mitigación

1.- Configurar la autenticación basada en certificados. Modifique el perfil VPN de RA para que requiera autenticación basada en certificados. Cuando se requiere la autenticación del certificado, Secure Access realiza una comprobación del certificado anteriormente en el flujo de autenticación. Si falta el certificado, el sistema produce un error antes del flujo de autenticación estándar y los eventos de "autorización fallida" no se registran de la misma manera.

2.- Validar la efectividad de la mitigación. Supervise los registros de autenticación después de implementar la autenticación basada en certificados para confirmar la reducción de eventos de autenticación excesivos. El cambio a la autenticación basada en certificados mitigó correctamente los ataques y redujo el ruido de registro.

Mejoras a largo plazo

Se crearon dos solicitudes de características para solucionar los problemas subyacentes:

- Solicitud de característica 1: Agregue una opción para ocultar o mostrar la lista de grupos de túnel (perfil VPN) cuando se agrega un arrendatario de VPN pública, lo que reduce la capacidad de detección de perfiles.
- Solicitud de característica 2: Agregue una opción de configuración para habilitar o deshabilitar el registro de intentos fallidos de autorización de VPN de RA, proporcionando a los administradores control sobre la amplitud del registro.

Además, se crea un documento público para explicar los eventos registrados y el comportamiento de autenticación para ayudar a los administradores a comprender las operaciones normales del sistema.

Causa

La causa raíz de los eventos de autenticación excesivos es la combinación de perfiles de VPN detectables en configuraciones de arrendatarios públicos y el comportamiento del flujo de autenticación cuando no se requiere autenticación basada en certificados. Cuando se utiliza la autenticación basada en RADIUS sin requisitos de certificado, el sistema registra todos los intentos de "autorización fallida" como parte de su condición de seguridad, incluidos los intentos de actores externos que descubren los perfiles VPN. Las direcciones locales de link en los registros representan el comportamiento normal del sistema interno para el proceso de autorización de cabecera de VPN de RA, no errores de configuración.

Contenido relacionado

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).