

Eventos de Autenticação de VPN RA de Acesso Seguro com Endereços de Servidor AAA de Link Local

Contents

Problema

Ao testar a funcionalidade de VPN do Acesso Remoto Seguro (RA), eventos de autenticação excessivos são registrados para identidades que não existem na organização do locatário. Os logs de autenticação mostram mais de 10.000 eventos de autenticação de VPN RA em um período de 24 horas, contendo erros de AAA como "AAALOG_SERVICE_DOWN" e "AAALOG_SERVER_DOWN". Essas mensagens de erro fazem referência a endereços link-local 169.254.x.x como o servidor AAA, que não estão configurados no espaço.

Exemplos de erros específicos observados nos registros incluem:

```
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
```

A atividade parece ser repetida em tentativas de autenticação baseadas em RADIUS contra o FQDN da VPN de Acesso Seguro, criando excesso de ruído de registro e levantando preocupações sobre varredura externa ou possível abuso do serviço VPN.

Ambiente

- Plataforma Cisco Secure Access
- Perfil de VPN de acesso remoto inicialmente configurado sem autenticação de certificado

- Autenticação baseada em RADIUS configurada para VPN RA
- Configuração de locatário de VPN pública com perfis de VPN detectáveis

Resolução

A resolução envolvia a compreensão do comportamento do fluxo de autenticação e a implementação da autenticação baseada em certificado como uma estratégia de mitigação.

Explicação técnica do comportamento observado

Os eventos de autenticação excessivos ocorrem devido aos motivos técnicos descritos nas próximas seções.

Fluxo de autenticação sem requisitos de certificado

Quando a autenticação de certificado é desativada e a autenticação de VPN RA baseada em RADIUS é usada, o sistema registra as tentativas de "falha de autorização" porque primeiro verifica a identidade do nome de usuário em relação ao banco de dados de usuários sincronizados no Secure Access e registra o evento de "falha de autorização". Esses eventos são esperados como uma primeira linha de defesa, mas podem produzir um ruído de registro significativo quando agentes externos tentam a autenticação.

Uso do endereço de link local

Os endereços 169.254.x.x vistos nos logs são endereços de link local/interno usados pelo headend da VPN do RA para autorizar sessões de entrada. Esses endereços representam o comportamento interno do sistema, em vez da configuração incorreta de servidores AAA no espaço.

Descoberta de Perfil VPN

Quando uma ID de locatário de VPN pública é configurada, os perfis de VPN são listados no menu suspenso de IU, o que pode permitir que agentes externos descubram perfis públicos mais facilmente e os direcionem para tentativas de autenticação.

Etapas de mitigação imediatas

1.- Configure a autenticação baseada em certificado. Modifique o perfil de VPN do RA para exigir autenticação baseada em certificado. Quando a autenticação de certificado é necessária, o Secure Access executa uma verificação de certificado antes do fluxo de autenticação. Se o certificado estiver ausente, o sistema produzirá um erro antes do fluxo de autenticação padrão e os eventos de "falha de autorização" não serão registrados da mesma maneira.

2.- Validar a eficácia da mitigação. Monitore os logs de autenticação após implementar a autenticação baseada em certificado para confirmar a redução no excesso de eventos de autenticação. A alternância para a autenticação baseada em certificado reduziu com êxito os ataques e o ruído de registro.

Melhorias a longo prazo

Duas solicitações de recursos foram criadas para resolver os problemas subjacentes:

- Solicitação de recurso 1: Adicione uma opção para ocultar ou mostrar a lista do grupo de túneis (perfil VPN) quando um locatário VPN público for adicionado, reduzindo a capacidade de descoberta de perfil.
- Solicitação de recurso 2: Adicione uma opção de configuração para habilitar ou desabilitar o log de tentativas de autorização de VPN RA com falha, fornecendo aos administradores o controle sobre o detalhamento do log.

Além disso, um documento voltado ao público é criado para explicar os eventos registrados e o comportamento de autenticação para ajudar os administradores a entender as operações normais do sistema.

Causa

A causa raiz dos eventos de autenticação excessivos é a combinação de perfis de VPN detectáveis em configurações de locatário público e o comportamento do fluxo de autenticação quando a autenticação baseada em certificado não é necessária. Quando a autenticação baseada em RADIUS é usada sem requisitos de certificado, o sistema registra todas as tentativas de "autorização com falha" como parte de sua postura de segurança, incluindo tentativas de agentes externos que descobrem os perfis de VPN. Os endereços de link local nos registros representam o comportamento interno normal do sistema para o processo de autorização de headend da VPN do RA, não erros de configuração.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.