

Falha de login da GUI de administração do ISE com o token RADIUS de federação PingID

Contents

Problema

O login da GUI do administrador no Cisco ISE falha ao usar a federação de PingID como um token RADIUS, apesar das capturas de pacotes que mostram que o Ping Federate retorna uma resposta de aceitação de acesso. A falha de login ocorre mesmo que a autenticação RADIUS pareça bem-sucedida de uma perspectiva de rede, impedindo o acesso administrativo à interface do ISE. A análise de pacote de rede confirma que o servidor PingID (10.32.154.200) envia a resposta Access-Accept esperada para o ISE (10.2.200.241), mas o processo de login do administrador do ISE ainda não foi concluído com êxito.

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.3 Patch 7
- Implantação de VM de 4 nós
- Federação PingID configurada como autenticação de token RADIUS
- Endereço IP do ISE: 10.2.200.241
- Endereço IP do servidor PingID: 10.32.154.200
- Configuração de Acesso de Administrador revisada em Administração > Acesso de Administrador

Resolução

O problema foi resolvido com a aplicação de uma solução alternativa que habilitou a

funcionalidade de login de administrador bem-sucedida. As etapas descritas nas próximas seções foram seguidas para solucionar o problema.

Passo 1: Coleta e análise de evidências

A evidência de captura de pacote foi coletada e analisada para confirmar o fluxo de autenticação RADIUS entre o ISE e o servidor PingID. A análise verificou se o ping federado estava enviando corretamente as respostas de aceitação de acesso.

Passo 2: Evidência de prt-server.log

##

prt-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

##

Passo 3: O que é o Autenticador de Mensagens?

O Autenticador de Mensagens é um atributo de segurança usado em pacotes RADIUS para garantir a integridade e a autenticidade das mensagens trocadas entre os dispositivos de rede e o servidor RADIUS. É uma assinatura criptográfica computada usando HMAC-MD5 sobre todo o pacote RADIUS com uma chave secreta compartilhada. Esse atributo ajuda a proteger contra adulteração e falsificação de mensagens RADIUS, especialmente aquelas que envolvem fluxos de autenticação do EAP (Extensible Authentication Protocol).

Passo 4: Implementação alternativa

Desabilitar "Autenticador de Mensagem Necessário na Resposta": Administração / Gerenciamento de identidade / Fontes de identidade externas / Token RADIUS. Clique no nome do Token RADIUS e vá para Authentication. Desmarque "Message Authenticator Required On Response".

Passo 5: Teste de validação

Após aplicar a solução, testes de login de administrador foram executados para validar a resolução. Esses testes confirmaram a autenticação e o acesso bem-sucedidos à GUI do administrador do ISE usando a federação PingID como o token RADIUS.

Passo 6: Período de monitoramento

Foi estabelecido um período de monitoramento e validação para garantir a estabilidade da solução alternativa. Durante esse período, foi realizado um teste de login administrativo contínuo sem erros ou falhas relatadas.

Causa

A falha de login da GUI do administrador do ISE foi causada por uma incompatibilidade de aplicação de segurança do protocolo RADIUS entre o Cisco ISE 3.3 Patch 7 e o PingID (Ping Federate) durante a autenticação MFA.

Especificamente:

- O Cisco ISE exigiu que o atributo `Message-Authenticator` do RADIUS estivesse presente na resposta `Access-Accept` do servidor de token RADIUS externo.
- PingID estava retornando respostas `Access-Accept` sem o atributo `Message-Authenticator`.
- Como o ISE tinha a configuração `Message Authenticator Required On Response` habilitada, ele silenciosamente rejeitou a resposta RADIUS como inválida, mesmo que a própria autenticação tenha sido bem-sucedida no lado do PingID.
- Essa aplicação faz parte do fortalecimento da segurança do Cisco ISE para mitigar a vulnerabilidade do Blast-RADIUS (CVE-2024-3596).

Conteúdo relacionado

- [Mitigação de Falsificação de Protocolo Blast-RADIUS \(CVE-2024-3596\)](#)

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.