Os usuários alertaram para a autenticação quando SaaS com fornecedor da identidade iniciou fluxos e NTLM

Índice

Pergunta

Por que os usuários são alertados para a autenticação quando SaaS com fornecedor da identidade iniciou fluxos e NTLM?

Ambiente

- Versões 7.0 ou mais recente sendo executado de AsyncOS da ferramenta de segurança da Web de Cisco (WSA)
- NTLM usado para a autenticação transparente
- Controle de acesso de SaaS configurado usando o fluxo iniciado identidade-fornecedor
- SaaS SSO configurado

Eu tenho o controle de acesso de SaaS configurado com meu aplicativo externo, usando o fluxo fornecedor-iniciado identidade e SAML para único sinal-em. Eu igualmente estou usando o NTLM para autenticar transparentemente meus usuários. Contudo, como posso eu impedir que ver esta alerta?

Sintomas

- Quando os usuários clicam sobre seu endereço da Internet para o SaaS SSO URL, veem às vezes as alertas da autenticação.
- Alcance trabalhos muito bem se os usuários alcançam uma outra site da web externo e clicam então o endereço da Internet de SaaS SSO URL.

Este problema ocorre quando/porque o primeiro pedido que o WSA vê do cliente é ao SSO especial URL, que está servido diretamente do WSA.

O índice que é servido diretamente do WSA - tal como páginas EUN ou arquivos PAC - é

normalmente isento da autenticação. Quando a característica de SaaS puder alcançar os substitutos da autenticação mantidos pelo proxy, não pode própria autenticação do pedido usando nenhum método além da autenticação formulário-baseada (NTLM ou LDAP). Assim o comportamento observado é pelo projeto mas não é uma solução ótima.

O defeito CSCzv55859 é arquivado para seguir este problema e para fornecer um mecanismo melhor para endereçar esta edição.

Há duas ações alternativas disponíveis.

Workaround 1

1. O primeiro é usar um fluxo Fornecedor-iniciado serviço na configuração de SaaS. Em um fluxo SP-iniciado, o usuário começa consultando ao aplicativo de SaaS do alvo, que emite então a reorientação com o SSO URL.
   Porque este tráfego inicial atravessa o proxy, o usuário obterá autenticado corretamente usando o NTLM. Esta ação alternativa trabalha somente se as sustentações do aplicativo do alvo SP-iniciaram fluxos.
2. Crie um SSO novo URL na política WSA, forçando a autenticação e reorientando então o cliente ao SSO “real” URL.

Workaround 2

1. Decida em um SSO novo URL. Esta URL será alcançada nunca realmente pelo proxy; atuará simplesmente como um ponto para iniciar sinal-no processo.

   Por exemplo, se o SSO atual URL é “**wsa.mycompany.com/SSOURL/WebEx**”, você pode usar “**wsa.example.com/SSOURL/WebEx**”.A consideração importante está certificando-se que a parcela que do hostname você se usa proxied com o WSA.

   Quando o WSA é distribuído como um proxy explícito, o hostname pode ser apenas sobre qualquer coisa.Se o WSA é distribuído como um proxy transparente, a seguir o hostname precisará de ser um hostname real que resolva a um endereço IP externo.

2. Crie uma categoria do costume URL (**GUI > gerenciador de segurança da Web > categorias feitas sob encomenda URL**) que combine o URL.You novo precise de criar uma categoria feita sob encomenda URL para cada aplicativo que de SaaS você precisa de aplicar a ação alternativa a.
   Use o fósforo da expressão regular para combinar na URL completa.

3. Vá às políticas de acesso (**GUI > gerenciador de segurança > políticas de acesso da Web**) e sob a coluna da Filtragem URL para uma política de acesso que o pedido de usuário combine. Esta pode ser a política global ou uma outra política mais cedo na tabela.
   Inclua a categoria nova do costume URL nesta política de acesso, e ajuste sua ação **para reorientar**. O alvo da reorientação deve ser o SSO “real” URL.

4. Submeta e comprometa as mudanças para aplicar a configuração nova.

Os usuários devem agora usar o SSO novo URL para alcançar o aplicativo. Porque o acesso a esta URL é processado pelo proxy, a autenticação de NTLM será invocada e o usuário seja sempre será assinado dentro transparentemente, evitando a autenticação alerta.