O AUTH falha com WSA quando o cliente usa NEGOEXTS

Índice

[Introdução](#)
[Informações de Apoio](#)
[Problema: O AUTH falha com WSA quando o cliente usa NEGOEXTS](#)
[Solução](#)

Introdução

Este documento descreve como ao overocme a edição quando o AUTH falha através da ferramenta de segurança da Web de Cisco (WSA) quando o cliente usa NEGOEXTS.

Informações de Apoio

A ferramenta de segurança da Web de Cisco (WSA) pode autenticar usuários para aplicar as políticas baseadas no usuário ou no grupo. Um dos métodos que está disponível é Kerberos. Ao usar o Kerberos como um método de autenticação em uma identidade, o WSA responde ao pedido do HTTP de um cliente com uns 401 (transparentes) ou a resposta HTTP 407 (explícita) que contém o encabeçamento WWW-**autentica: Negocie**. Neste momento, o cliente envia um pedido do HTTP novo com a **autorização: Negocie o** encabeçamento, que contém o Application Program Interface genérico do serviço de segurança (GSS-API) e protocolos protegidos simples da negociação (SPNEGO). Sob SPNEGO, o usuário apresenta os **mechTypes** que apoia. Estes são os mechTypes que WSA apoia:

- KRB5- o método do AUTH do Kerberos que está usado se o Kerberos está apoiado e configurado corretamente no cliente e se um bilhete válido do Kerberos esta presente para o serviço que está sendo alcançado
- NTLMSSP- o provedor de suporte de segurança que de Microsoft NTLM o método que é usado se nenhum bilhete válido do Kerberos está disponível mas negocia o método do AUTH é apoiado

Problema: O AUTH falha com WSA quando o cliente usa NEGOEXTS

Em mais versões recentes de Microsoft Windows, um método novo do AUTH é apoiado chamou NegoExts, que é uma extensão ao protocolo de autenticação do negócio. Este mechType está considerado mais seguro do que NTLMSSP, e preferido pelo cliente quando os únicos métodos suportados são NEGOEXTS e NTLMSSP. Mais informação pode ser encontrada neste link:

[Introduzindo Ramais ao pacote da autenticação do negócio](#)

Esta encenação ocorre tipicamente quando o método do AUTH do negócio é selecionado e não

há nenhum mechType KRB5 (muito provavelmente devido a faltar um bilhete válido do Kerberos para o serviço WSA). Se o cliente seleciona NEGOEXTS (pode ser visto como NEGOEX no wireshark), a seguir o WSA unabled para processar a transação do AUTH e o AUTH falha para o cliente. Quando isto ocorre, estes logs estão considerados nos logs do AUTH:

```
14 Nov 2016 16:06:20 (GMT -0500) Warning: PROX_AUTH : 123858 : [DOMAIN]Failed to parse NTLMSSP
packet, could not extract NTLMSSP command14 Nov 2016 16:06:20 (GMT -0500) Info: PROX_AUTH :
123858 : [DOMAIN][000] 4E 45 47 4F 45 58 54 53 00 00 00 00 00 00 00 00 NEGOEXTS ........
```

Quando o AUTH falha, este ocorre:

Se os privilégios do convidado são permitidos - o cliente está classificado como **não-autenticado** e reorientado ao Web site

Se os privilégios do convidado são desabilitados - o cliente é presentado com uns outros 401 ou 407 (segundo o método do proxy) com os métodos restantes do AUTH apresentados no cabeçalho da resposta (Negotiate não é apresentado outra vez). Uma alerta do AUTH é provável ser ocorrida se NTLMSSP e/ou o AUTH básico são configurados. Se não há nenhum outro método do AUTH (a identidade está configurada somente para o Kerberos), a seguir o AUTH falha simplesmente.

Solução

A solução a esta edição está a ou remove o AUTH do Kerberos da identidade - ou fixa o cliente de modo que obtenha um bilhete válido do Kerberos para o serviço WSA.