Auténtico falla con WSA cuando el cliente utiliza NEGOEXTS

Contenido

Introducción

Este documento describe cómo al overocme el problema cuando es auténtico falla a través del dispositivo de seguridad de la red de Cisco (WSA) cuando el cliente utiliza NEGOEXTS.

Antecedentes

El dispositivo de seguridad de la red de Cisco (WSA) puede autenticar a los usuarios para aplicar las directivas basadas en el usuario o el grupo. Uno de los métodos que está disponible es Kerberos. Al usar el Kerberos como método de autenticación en una identidad, el WSA contesta a la solicitud HTTP de un cliente con 401 (transparentes) o 407 HTTP de respuestas (explícitos) que contiene la encabezado WWW-**autentican: Negocie**. A este punto, el cliente envía una nueva solicitud HTTP con la **autorización: Negocie la** encabezado, que contiene la interfaz de programación de aplicaciones genérica del servicio de seguridad (GSS API) y los protocolos protegidos simples de la negociación (SPNEGO). Bajo SPNEGO, el usuario presenta los **mechTypes** que utiliza. Éstos son los mechTypes que WSA utiliza:

- KRB5- el método auténtico del Kerberos se utiliza que si el Kerberos se utiliza y se configura correctamente en el cliente y si un boleto válido del Kerberos está presente para el servicio que es alcanzado
- NTLMSSP- se utiliza el proveedor de compatibilidad para seguridad NTLM de Microsoft que el método se utiliza que si no hay boletos válidos del Kerberos disponibles pero negocia el método auténtico

Problema: Auténtico falla con WSA cuando el cliente utiliza NEGOEXTS

En más versiones recientes de Microsoft Windows, se utiliza un nuevo método auténtico llamó NegoExts, que es una extensión al protocolo de autenticación de la negociación. Este mechType se considera más seguro que NTLMSSP, y es preferido por el cliente cuando los únicos métodos aceptados son NEGOEXTS y NTLMSSP. Más información se puede encontrar en este link:

Introducción de las Extensiones al paquete de la autenticación de la negociación

Este decorado ocurre típicamente cuando se selecciona el método auténtico de la negociación y

no hay mechType KRB5 (muy probablemente debido a faltar un boleto válido del Kerberos para el servicio WSA). Si el cliente selecciona NEGOEXTS (puede ser visto como NEGOEX en el wireshark), después el WSA unabled para procesar la transacción auténtica y auténtico falla para el cliente. Cuando ocurre esto, estos registros se ven en los registros auténticos:

```
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 ........
```

Cuando es auténtico falla, esto ocurre:

Si se activan los privilegios del invitado - clasifican como **Unauthenticated** y se reorientan al cliente al sitio web

Si se inhabilitan los privilegios del invitado - presentan el cliente con otros 401 o 407 (dependiendo del método del proxy) con los métodos auténticos restantes presentados en el encabezado de respuesta (Negotiate no se presenta otra vez). Un mensaje auténtico es probable ser ocurrido si se configura NTLMSSP y/o auténtico básico. Si hay no otros métodos auténticos (la identidad se configura solamente para el Kerberos), después auténtico falla simplemente.

Solución

La solución a este problema está a o quita el Kerberos auténtico de la identidad - o fija al cliente de modo que consiga un boleto válido del Kerberos para el servicio WSA.