Autenticazione non riuscita tramite WSA quando il client utilizza NEGOEXTS

Sommario

Introduzione

In questo documento viene descritto come risolvere il problema quando l'autenticazione non riesce tramite Cisco Web Security Appliance (WSA) quando il client utilizza NEGOEXTS.

Premesse

Cisco Web Security Appliance (WSA) può autenticare gli utenti per applicare le policy in base all'utente o al gruppo. Uno dei metodi disponibili è Kerberos. Quando si utilizza Kerberos come metodo di autenticazione in un oggetto Identity, il server WSA risponde alla richiesta HTTP di un client con una risposta HTTP 401 (trasparente) o 407 (esplicita) contenente l'intestazione **WWW-Authenticate: Negoziare**. A questo punto, il client invia una nuova richiesta HTTP con il messaggio di **autorizzazione:** Intestazione **Negotiate**, contenente i protocolli GSS-API (Generic Security Service Application Program Interface) e SPNEGO (Simple Protected Negotation). In SPNEGO, l'utente presenta i **mechTypes** supportati. MechTypes supportati da WSA:

- KRB5 - Metodo di autenticazione Kerberos utilizzato se Kerberos è supportato e configurato correttamente nel client e se è presente un ticket Kerberos valido per il servizio a cui si accede
- NTLMSSP: metodo del provider di supporto della sicurezza NTLM di Microsoft utilizzato se non sono disponibili ticket Kerberos validi ma è supportato il metodo di autenticazione Negotiate.

Problema: Auth non riuscito tramite WSA quando il client utilizza NEGOEXTS

Nelle versioni più recenti di Microsoft Windows è supportato un nuovo metodo di autenticazione denominato NegoExts, che è un'estensione del protocollo di autenticazione Negotiate. Questo mechType è considerato più sicuro di NTLMSSP ed è preferito dal client quando gli unici metodi supportati sono NEGOEXTS e NTLMSSP. Per ulteriori informazioni, visitare questo link:

[Introduzione alle estensioni del pacchetto di autenticazione Negotiate](#)

Questo scenario si verifica in genere quando viene selezionato il metodo di autenticazione Negotiate e non è presente alcun mechType KRB5 (molto probabilmente a causa della mancanza

di un ticket Kerberos valido per il servizio WSA). Se il client seleziona NEGOEXTS (può essere visto come NEGOEX in wireshark), WSA non è in grado di elaborare la transazione di autenticazione e l'autenticazione non riesce per il client. In questo caso, i seguenti log vengono visualizzati nei log di autenticazione:

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

Se l'autenticazione non riesce, si verifica quanto segue:

Se i privilegi guest sono abilitati, il client viene classificato come non autenticato e reindirizzato al sito Web

Se i privilegi guest sono disabilitati, al client viene presentato un altro 401 o 407 (a seconda del metodo proxy) con i restanti metodi di autenticazione presentati nell'intestazione della risposta (Negotiate non viene più presentato). Se si configura l'autenticazione NTLMSSP e/o di base, è probabile che venga visualizzato un prompt di autenticazione. Se non sono disponibili altri metodi di autenticazione (l'identità è configurata solo per Kerberos), l'autenticazione avrà esito negativo.

Soluzione

Per risolvere il problema, rimuovere l'autorizzazione Kerberos dall'identità oppure correggere il client in modo che ottenga un ticket Kerberos valido per il servizio WSA.