Auth heeft geen invloed op WSA wanneer client NEGOEXTS gebruikt

Inhoud

Inleiding

Dit document beschrijft hoe de kwestie te overwinnen wanneer Auth faalt door Cisco Web Security Appliance (WSA) wanneer de client NEGOEXTS gebruikt.

Achtergrondinformatie

De Cisco Web Security Appliance (WSA) kan gebruikers voor authenticatie behoeden om beleid toe te passen op basis van gebruiker of groep. Een van de beschikbare methoden is Kerberos. Wanneer Kerberos als authenticatiemethode in een Identity wordt gebruikt, reageert de WSA op een HTTP-aanvraag van een client met een 401 (transparant) of 407 (expliciet) HTTP-respons die de header **WWW-Authenticate** bevat**: Onderhandelen**. Op dit moment stuurt de client een nieuw HTTP-verzoek met de **autorisatie: Onderhandelingen** over de header, die de Generic Security Service Application Program Interface (GSS-API) en Simple Protected Negation (SPNEGO) protocollen bevat. Onder SPNEGO presenteert de gebruiker de **technische** types die het ondersteunt. Dit zijn de technische types die WSA ondersteunt:

- KRB5-Kerberos auth-methode die wordt gebruikt als Kerberos op de client correct wordt ondersteund en ingesteld en als er een geldig Kerberos-ticket aanwezig is voor de service die toegankelijk is
- NTLMSSP - Microsoft NTLM Security Support Provider-methode die wordt gebruikt indien er geen geldige Kerberos-tickets beschikbaar zijn, maar de onderhandelings-automatiseringsmethode wordt ondersteund

Probleem: Auth Failover door WSA wanneer client NEGOEXTS gebruikt

In recenter versies van Microsoft Windows wordt een nieuwe autemethode ondersteund die NegoExts wordt genoemd, wat een uitbreiding is van het protocol voor de verificatie van onderhandelingen. Dit technische type wordt als veiliger dan NTLMSSP beschouwd en wordt door de klant geprefereerd wanneer de enige ondersteunde methoden NEGOEXTS en NTLMSSP zijn. Meer informatie is te vinden op deze link :

[Inleiding over uitbreidingen van het onderhandelingspakket voor verificatie](#)

Dit scenario doet zich doorgaans voor wanneer de methode van de onderhandelingsvergunning is geselecteerd en er geen MechType van KRB5 is (waarschijnlijk door het ontbreken van een geldig Kerberos Ticket voor de WSA-dienst). Als de client NEGOEXTS selecteert (dit kan worden gezien als NEGOEX in wireshark) is de WSA niet in staat om de auth transactions te verwerken en de auth error voor de client. Wanneer dit voorkomt, worden deze logs gezien in de auth logs:

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

Wanneer auth faalt, gebeurt dit:

Als gastenrechten zijn ingeschakeld, wordt client geclassificeerd als **ongeëigend** en wordt hij doorverwezen naar de website

Indien de gastarbevoorrechten worden uitgeschakeld - de klant krijgt 401 of 407 extra rechten (afhankelijk van de methode bij volmacht) met de resterende controlemethoden die in de antwoordheader worden voorgesteld (onderhandeling wordt niet opnieuw gepresenteerd). Een auth-prompt wordt waarschijnlijk uitgevoerd als NTLMSSP en/of Basic-auth is ingesteld. Als er geen andere auth methods zijn (Identity is alleen ingesteld voor Kerberos), dan zal de auth simpelweg mislukken.

Oplossing

De oplossing voor deze kwestie is om of Kerberos auth van de Identiteit te verwijderen of - de client te repareren zodat het een geldig Kerberos ticket voor de WSA dienst krijgt.