Auth schlägt durch WSA fehl, wenn der Client NEGOEXTS verwendet

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie das Problem behoben wird, wenn Auth über die Cisco Web Security Appliance (WSA) ausfällt, wenn der Client NEGOEXTS verwendet.

Hintergrundinformationen

Die Cisco Web Security Appliance (WSA) kann Benutzer authentifizieren, um Richtlinien basierend auf Benutzer oder Gruppen anzuwenden. Eine der verfügbaren Methoden ist Kerberos. Wenn Kerberos als Authentifizierungsmethode in einer Identität verwendet wird, antwortet die WSA auf die HTTP-Anfrage eines Clients mit einer 401 (transparenten) oder 407 (expliziten) HTTP-Antwort, die den Header **WWW-Authenticate** enthält**: Verhandeln**. An diesem Punkt sendet der Client eine neue HTTP-Anfrage mit der **Autorisierung: Negotiate**-Header, der die Protokolle Generic Security Service Application Program Interface (GSS-API) und Simple Protected Negotiation (SPNEGO) enthält. Unter SPNEGO zeigt der Benutzer die unterstützten **mechTypes** an. Diese mechTypes werden von der WSA unterstützt:

- KRB5- Kerberos-Authentifizierungsmethode, die verwendet wird, wenn Kerberos auf dem Client unterstützt und korrekt konfiguriert wird und wenn ein gültiges Kerberos-Ticket vorhanden ist, auf das zugegriffen wird
- NTLMSSP - Microsoft NTLM Security Support Provider-Methode, die verwendet wird, wenn keine gültigen Kerberos-Tickets verfügbar sind, die Negotiate-Authentifizierungsmethode jedoch unterstützt wird

Problem: Auth schlägt durch WSA fehl, wenn der Client NEGOEXTS verwendet

In neueren Versionen von Microsoft Windows wird eine neue Authentifizierungsmethode mit dem Namen NegoExts unterstützt, eine Erweiterung des Authentifizierungsprotokolls Negotiate. Dieser mechType gilt als sicherer als NTLMSSP und wird vom Client bevorzugt, wenn NEGOEXTS und NTLMSSP die einzigen unterstützten Methoden sind. Weitere Informationen finden Sie unter:

[Einführung von Erweiterungen in das Verhandlungspaket](#)

Dieses Szenario tritt in der Regel ein, wenn die Negotiate-Authentifizierungsmethode ausgewählt

wird und kein KRB5 mechType vorhanden ist (höchstwahrscheinlich, weil ein gültiges Kerberos-Ticket für den WSA-Dienst fehlt). Wenn der Client NEGOEXTS auswählt (in Wireshark als NEGOEX angesehen werden kann), ist die WSA nicht für die Verarbeitung der Authentifizierungstransaktion aktiviert, und die Autorisierung schlägt für den Client fehl. In diesem Fall werden diese Protokolle in den Authentifizierungsprotokollen angezeigt:

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

Wenn die Authentifizierung fehlschlägt, geschieht Folgendes:

Wenn Gastberechtigungen aktiviert sind, wird der Client als **nicht authentifiziert** und an die Website weitergeleitet.

Wenn Gastberechtigungen deaktiviert sind, werden dem Client weitere 401 oder 407 angezeigt (je nach Proxymethode), wobei die verbleibenden Authentifizierungsmethoden im Antwortheader dargestellt werden (Negotiate wird nicht erneut angezeigt). Wenn NTLMSSP und/oder die Basic-Authentifizierung konfiguriert ist, ist eine Eingabeaufforderung wahrscheinlich vorhanden. Wenn es keine anderen Authentifizierungsmethoden gibt (Identität wird nur für Kerberos konfiguriert), schlägt die Authentifizierung einfach fehl.

Lösung

Die Lösung für dieses Problem besteht darin, die Kerberos-Authentifizierung entweder aus der Identität zu entfernen - oder - den Client zu reparieren, damit er ein gültiges Kerberos-Ticket für den WSA-Service erhält.