Datenverkehr von Windows 7-/Vista-Clients zeigt Workstation statt Benutzer in den Zugriffsprotokollen an

Inhalt

Frage

Warum zeigt der Datenverkehr von Windows 7-/Vista-Clients in den Zugriffsprotokollen Workstations statt Benutzer an?

Umgebung

Microsoft Windows 7, Microsoft Windows Vista, Cisco Web Security Appliance (alle Versionen), Surrogattyp: IP-Adresse

Symptome

Bestimmte Protokollzeilen in den Zugriffsprotokollen zeigen den Computernamen anstelle von DOMÄNE\USER an.

Microsoft hat eine neue Funktion in Windows 7 und Windows Vista eingeführt, die als "Network Connectivity Status Indicator" (NCSI) bezeichnet wird und als kleines globales Symbol angezeigt wird, das im Systembereich über das Symbol für die Netzwerkschnittstelle angezeigt wird. Unmittelbar nach der Anmeldung versucht diese Funktion, Daten aus dem Internet anzufordern, um festzustellen, ob eine Internetverbindung besteht.

Es sind Probleme mit NCSI bekannt, bei denen NCSI Anmeldeinformationen anstatt Benutzeranmeldeinformationen sendet, wenn eine NTLM-Authentifizierung erforderlich ist.

Da NCSI höchstwahrscheinlich die erste Anforderung von einem PC an die WSA sendet, existiert noch kein Ersatzgerät, und es wird ein neues IP-basiertes Ersatzgerät mit dem Computernamen anstelle des tatsächlichen Benutzernamens erstellt. Dieses Ersatzzeichen wird für jede Anforderung von der ursprünglichen IP-Adresse bis zur Zeitüberschreitung beim Surrogat verwendet und der Benutzer muss sich erneut authentifizieren, dieses Mal mit echten Anmeldeinformationen.

Da der Computername höchstwahrscheinlich kein Mitglied der ursprünglich beabsichtigten AD-Gruppe ist, werden bei allen Anfragen nicht die richtigen Zugriffs-/Entschlüsselungsrichtlinien ausgelöst, was manchmal dazu führt, dass die Anforderung blockiert wird.

Weitere Informationen zu NCSI finden Sie im folgenden Microsoft KB-Artikel.

Bitte beachten Sie die unten stehenden Anweisungen, um das Problem zu umgehen:

1. Starten Sie den Registrierungs-Editor, indem Sie im Taskmenü nach "regedit" suchen. Klicken Sie mit der rechten Maustaste, und wählen Sie "Als Administrator ausführen" aus.

2. Navigieren Sie zu: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet

3. Doppelklicken Sie unter dem Internet-Schlüssel auf "EnableActiveProbing", und geben Sie dann unter "Value data" Folgendes ein: **0**.
4. Klicken Sie auf "OK".

5. Starten Sie den Computer neu.

Diese Änderungen können mithilfe des Domänencontrollers als Global Policy Object (GPO) an alle Clients übertragen werden.

Problemumgehung auf der WSA

Erstellen Sie eine Identität für NCSI, und nehmen Sie sie von der Authentifizierung auf Basis der URL oder des Benutzer-Agenten aus.

Bekannte URLs, mit denen NCSI verbunden ist

ncsi.glbdns.microsoft.com
newncsi.glbdns.microsoft.com
www.msftncsi.com

NCSI-Benutzer-Agent

Microsoft NCSI