L'accesso a un desktop remoto tramite RDP comporta la modifica dell'utente associato a un indirizzo IP

Sommario

Introduzione

Se si accede a un host remoto utilizzando il protocollo RDP (Remote Desktop Protocol) e il nome utente remoto è diverso da quello dell'utente, FireSIGHT System modifica l'indirizzo IP dell'utente associato all'indirizzo IP dell'utente nel centro di gestione FireSIGHT. Determina la modifica delle autorizzazioni per l'utente in relazione alle regole di controllo di accesso. Noterete cheL'utente non corretto è associato alla workstation. Questo documento offre una soluzione al problema.

Prerequisiti

Cisco raccomanda la conoscenza del sistema FireSIGHT e dell'agente utente.

> Nota: le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Causa principale

Questo problema si verifica a causa del modo in cui Microsoft Active Directory(AD) registra i tentativi di autenticazione RDP nei registri di sicurezza di Windows nel controller di dominio. AD registra il tentativo di autenticazione per la sessione RDP sull'indirizzo IP dell'host di origine

anziché sull'endpoint RDP a cui ci si sta connettendo. Se si accede all'host remoto con un account utente diverso, verrà modificato l'utente associato all'indirizzo IP della workstation originale.

Verifica

Per verificare questa condizione, è possibile verificare che l'indirizzo IP dell'evento di accesso della workstation originale e dell'host remoto RDP abbiano lo stesso indirizzo IP.

Per trovare questi eventi, è necessario seguire i seguenti passaggi:

Passaggio 1: Determinare il controller di dominio utilizzato dall'host per l'autenticazione:

Eseguire il comando seguente:

```
nltest /dsgetdc:<windows.domain.name>
```

Output di esempio:

```
C:\Users\WinXP.LAB>nltest /dsgetdc:support.lab
           DC: \\Win2k8.support.lab
      Address: \\192.X.X.X
     Dom Guid: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
     Dom Name: support.lab
  Forest Name: support.lab
 Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
        Flags: PDC GC DS LDAP KDC TIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST
 CLOSE_SITE FULL_SECRET WS 0x4000
The command completed successfully
```

La riga che inizia con "DC:" sarà il nome del controller di dominio e la riga che inizia con "Address:" sarà l'indirizzo IP.

Passaggio 2: utilizzo del log RDP nel controller di dominio identificato nel passaggio 1

Passaggio 3: selezionare Start > Strumenti di amministrazione > Visualizzatore eventi.

Passaggio 4: espandere Registri Windows > Protezione.

Passaggio 5: filtrare l'indirizzo IP della workstation facendo clic su Filtra registro corrente, quindi

sulla scheda XML e infine su Modifica query.

Passaggio 6: immettere la seguente query XML, sostituendo l'indirizzo IP con <indirizzo IP>

```
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">
*[EventData[Data[@Name='IpAddress'] and(Data='<IP address>')]]
</Select>
</Query>
</QueryList>
```

Passaggio 7: fare clic su Logon Event (Evento di accesso) e selezionare la scheda Details (Dettagli).

Un esempio di output:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Security-Auditing"
Guid="{XXXXXXXX-XXX-XXXX-XXX-XXXXXXXXXXXX}"/>
<EventID>4624</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2014-07-22T20:35:12.750Z" />
<EventRecordID>4130857</EventRecordID>
<Correlation />
<Execution ProcessID="576" ThreadID="704" />
<Channel>Security</Channel>
<Computer>WIN2k8.Support.lab</Computer>
<Security />
</System>
- <EventData>
<Data Name="SubjectUserSid">S-1-0-0</Data>
<Data Name="SubjectUserName">-</Data>
<Data Name="SubjectDomainName">-</Data>
<Data Name="SubjectLogonId">0x0</Data>
<Data Name="TargetUserSid">S-X-X-XX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXX-XXXX</Data>
<Data Name="TargetUserName">WINXP-SUPLAB$</Data>
<Data Name="TargetDomainName">SUPPORT</Data>
<Data Name="TargetLogonId">0x13c4101f</Data>
<Data Name="LogonType">3</Data>
<Data Name="LogonProcessName">Kerberos</Data>
<Data Name="AuthenticationPackageName">Kerberos</Data>
<Data Name="WorkstationName" />
<Data Name="LogonGuid">{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
```

```
<Data Name="ProcessId">0x0</Data>
<Data Name="ProcessName">-</Data>
<Data Name="IpAddress">192.0.2.10</Data>
<Data Name="IpPort">2401</Data>
</EventData>
```

Completare la stessa procedura dopo aver effettuato l'accesso tramite RDP e si noterà che si riceverà un altro evento di accesso (ID evento 4624) con lo stesso indirizzo IP mostrato dalla riga seguente dai dati XML dell'evento di accesso dall'accesso originale:

```
<Data Name="IpAddress">192.x.x.x</Data>
```

Soluzione

Per risolvere il problema, se si utilizza User Agent 2.1 o versione successiva, è possibile escludere tutti gli account che verranno
essere utilizzato principalmente per RDP nella configurazione dell'agente utente.

Passaggio 1: accedere all'host agente utente.

Passaggio 2: Avviare l'interfaccia utente di User Agent.

Passaggio 3: fare clic sulla scheda Nomi utente esclusi.

Passaggio 4: immettere tutti i nomi utente che si desidera escludere.

Passaggio 5: fare clic su Salva.

Gli utenti inseriti in questo elenco non generano eventi di accesso su FireSIGHT Management Center e non possono
associati a indirizzi IP.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).