Aanmelden bij een externe desktop met RDP wijzigt de gebruiker die is gekoppeld aan een IP-adres

Inhoud

Inleiding

Als u zich aanmeldt bij een externe host met Remote Desktop Protocol (RDP), en de externe gebruikersnaam verschilt van uw gebruiker, wijzigt FireSIGHT System het IP-adres van de gebruiker dat is gekoppeld aan uw IP-adres op het FireSIGHT Management Center. Het veroorzaakt verandering in de rechten van de gebruiker met betrekking tot de toegangscontroleregels. U zult merken datOnjuiste gebruiker is gekoppeld aan werkstation. Dit document biedt een oplossing voor dit probleem.

Voorwaarden

Cisco raadt u aan kennis te hebben van FireSIGHT System en User Agent.

> **Opmerking**: de informatie in dit document is gemaakt van de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Hoofdoorzaak

Dit probleem doet zich voor door de manier waarop Microsoft Active Directory (AD) RDP-verificatie probeert te koppelen aan de Windows Security Logs op de Domain Controller. AD registreert de verificatiepoging voor de RDP-sessie tegen het IP-adres van de oorspronkelijke host

in plaats van tegen het RDP-eindpunt waarmee u verbinding maakt. Als u zich aanmeldt bij de externe host met een andere gebruikersaccount, verandert dit de gebruiker die is gekoppeld aan het IP-adres van het oorspronkelijke werkstation.

Verificatie

Om te verifiëren dat dit is wat er gebeurt, kunt u verifiëren dat het IP-adres van de logon-gebeurtenis vanaf uw oorspronkelijke werkstation en de RDP-externe host hetzelfde IP-adres hebben.

Om deze gebeurtenissen te vinden, moet u de onderstaande stappen volgen:

Stap 1: Bepaal de Domeincontroller die u host wordt geverifieerd aan de hand van:

Voer de volgende opdracht uit:

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

Voorbeelduitvoer:

```
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
```

De regel die begint met "DC:" zal de naam zijn van de Domain Controller en de regel die begint met "Address:" zal het IP-adres zijn.

Stap 2: Het gebruik van RDP-logbestand in de domeincontroller die in stap 1 is geïdentificeerd

Stap 3: Ga naar **Start > Administratieve tools > Event Viewer**.

Stap 4: Boor neer aan de **Logboeken van Windows > Veiligheid**.

Stap 5: Filter voor het IP-adres van uw werkstation door op Filter Current Log te klikken, op het tabblad XML te klikken en op query bewerken te klikken.

Stap 6: Voer de volgende XML-query in en vervang uw IP-adres door **<ip-adres>**

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

Stap 7: Klik op de **Logon Event** en klik op het tabblad **Details**.

Een voorbeeld van uitvoer:

```
- <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>
```

Voltooi deze zelfde stappen na het inloggen via RDP en u zult merken dat u een andere inloggebeurtenis (gebeurtenis-ID 4624) met hetzelfde IP-adres ontvangen zoals getoond door de volgende regel van de inloggebeurtenis XML-gegevens van de oorspronkelijke inlogdatum:

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

Oplossing

Om dit probleem te verhelpen, kunt u, als u Gebruikersagent 2.1 of hoger gebruikt, alle accounts uitsluiten die u wilt
voornamelijk voor RDP worden gebruikt in de configuratie van de User Agent.

Stap 1: Log in op de User Agent-host.

Stap 2: Start de User Agent-gebruikersinterface.

Stap 3: Klik op het tabblad **Uitgesloten gebruikersnamen**.

Stap 4: Voer alle gebruikersnaam in die u wilt uitsluiten.

Stap 5: Klik op **Opslaan**.

Gebruikers die in deze lijst zijn ingevoerd, genereren geen aanmeldingsgebeurtenissen op het FireSIGHT Management Center en worden niet geautoriseerd
gekoppeld aan IP-adressen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.