使用RDP登入遠端案頭將更改與IP地址關聯的使用者

目錄

簡介

如果您使用遠端案頭協定(RDP)登入到遠端主機，並且遠端使用者名稱不同於您的使用者，則FireSIGHT系統將在FireSIGHT管理中心上更改與您的IP地址關聯的使用者的IP地址。這會導致使用者與訪問控制規則相關的許可權發生更改。你會注意到我不正確的使用者與工作站關聯。本文提供此問題的解決方案。

必要條件

思科建議您瞭解FireSIGHT系統和使用者代理。

> **注意**：本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

根本原因

此問題是由於Microsoft Active Directory(AD)將RDP身份驗證嘗試記錄到域控制器上的Windows安全日誌的方式造成的。AD記錄針對始發主機IP地址而非RDP終端的RDP會話身份驗證嘗試。如果您使用不同的使用者帳戶登入到遠端主機，這將更改與原始工作站的IP地址關聯的使用者。

驗證

要驗證這是什麼情況，您可以驗證來自原始工作站的登入事件的IP地址與RDP遠端主機的IP地址是否相同。

要查詢這些事件，您需要執行以下步驟：

第1步：確定主機正在對其進行身份驗證的域控制器：

運行以下命令：

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

輸出示例：

```
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
```

啟動「DC：」的行將是域控制器的名稱，啟動「Address：」的行將是IP地址。

第2步：使用RDP登入到第1步中識別的域控制器

第3步：轉至**開始>管理工具>事件檢視器**。

第4步：細化到**Windows Logs > Security**。

第5步：通過按一下過濾當前日誌，按一下XML頁籤，然後按一下編輯查詢來過濾工作站的IP地址。

第6步：輸入以下XML查詢，將IP地址替換為<ip address>

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

第7步：按一下**Logon Event**，然後按一下**Details**頁籤。

輸出示例：

```
- <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>
```

在通過RDP登入後完成這些相同步驟，您會注意到您將收到另一個登入事件（事件ID 4624），該事件的IP地址與來自原始登入的登入事件XML資料中的以下行所示相同：

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

解決方案

要緩解此問題，如果您使用的是使用者代理2.1或更高版本，則可以排除您將要使用的任何帳戶主要用於使用者代理配置中的RDP。

第1步：登入到使用者代理主機。

第2步：啟動使用者代理使用者介面。

第3步：點選**Excluded Usernames**選項卡。

第4步：輸入要排除的所有使用者名稱。

第5步：按一下**Save**。

在此清單中輸入的使用者不會在FireSIGHT管理中心上生成登入事件，因此不會生成登入事件與IP地址關聯。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。