使用RDP登录远程桌面会更改与IP地址关联的用户

目录

简介

如果使用远程桌面协议(RDP)登录到远程主机，并且远程用户名不同于用户，则FireSIGHT系统将在FireSIGHT管理中心上更改与您的IP地址关联的用户的IP地址。这会导致用户相对于访问控制规则的权限发生更改。你会注意到不正确的用户与工作站关联。本文档提供了此问题的解决方案。

先决条件

Cisco建议您具备FireSIGHT系统和用户代理知识。

> **注意**：本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

根本原因

此问题是由于Microsoft Active Directory(AD)将RDP身份验证尝试记录到域控制器上的Windows安全日志的方式造成的。AD记录针对源主机IP地址（而不是您连接的RDP终端）的RDP会话身份验证尝试。如果您使用其他用户帐户登录到远程主机，这将更改与原始工作站的IP地址关联的用户。

确认

要验证这是什么情况，您可以验证来自原始工作站的登录事件的IP地址与RDP远程主机的IP地址是否相同。

要查找这些事件，您需要执行以下步骤：

第1步：确定主机针对哪个域控制器进行身份验证：

运行以下命令：

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

示例输出：

```
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
```

启动“DC：”的行将是域控制器的名称，启动“Address：”的行将是IP地址。

第2步：使用RDP登录第1步中识别的域控制器

第3步：转至**开始>管理工具>事件查看器**。

第4步：向下钻取到**Windows Logs > Security**。

第5步：点击过滤当前日志，点击XML选项卡，然后点击编辑查询，过滤工作站的IP地址。

第6步：输入以下XML查询，将IP地址替换为<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：单击**Logon Event**，然后单击**Details**选项卡。

输出示例：

```
- <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>
```

在通过RDP登录后完成这些相同的步骤，您会注意到您将从原始登录的登录事件XML数据收到具有如下所示相同IP地址的另一登录事件（事件ID 4624）：

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

解决方案

要缓解此问题，如果您使用的是用户代理2.1或更高版本，则可以排除您将要使用的任何帐户主要用于用户代理配置中的RDP。

第1步：登录用户代理主机。

第2步：启动用户代理用户界面。

第3步：点击**Excluded Usernames选**项卡。

第4步：输入要排除的所有用户名。

第5步：点击**保存**。

在此列表中输入的用户不会在FireSIGHT管理中心上生成登录事件，因此不会生成登录事件与IP地址相关联。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。