Обновление MS16-072 ломает Group Policy

По мотивам https://habrahabr.ru/post/304202/ и
http://winitpro.ru/index.php/2016/07/05/kak-izmenit-standartnye-razresheniya-dlya-novyx-gpo/

Обновление KB3163622 (бюллетень безопасности MS16-072, номер KB для различных ОС: KB3159398, KB3163017, KB3163018, KB3163016) ломает Group Policy. Выражается это в том, что GPO не применяются если в фильтре безопасности заданы группы или пользователи.

Как оказалось, для решения проблемы MitM программисты Microsoft не нашли ничего лучше, чем изменить поведение процесса применения групповых политик, которое не менялось со времени выхода Windows 2000. Традиционное поведение предусматривало доступ к политикам безопасности уровня компьютеров (computer scope) от учётной записи компьютера, а к политикам безопасности уровня пользователя (user scope) — от учётной записи пользователя. После установки обновления KB3163622 все запросы стали направляться от учётной записи компьютера, чтобы обеспечить доверенность источника силами протокола Kerberos.

Решение

Добавления разрешений на все объекты групповой политики

Это добавит права на текущие объекты GPO и они заработают правильно

Для английской версии:

```
> Get-GPO -All | Set-GPPermissions -TargetType Group -TargetName "Domain
Computers" -PermissionLevel GpoRead
```

Для русской версии:

```
> Get-GPO -All | Set-GPPermissions -TargetType Group -TargetName
"Компьютеры домена" -PermissionLevel GpoRead
```

Изменяем стандартные разрешения для новых GPO

- Запускаем ADSIEdit.msc и в открывшемся окне выбираем:
  - Английская версия: Action → «Connect to» и подключаемся к контексту схемы AD домена (Schema)
  - Русская версия: Действие → «Подключиться к» и подключаемся к контексту схемы AD домена: «Выберите известный контекст наименования» → Схема
- Разворачиваем схему, открываем имя CN=Group-Policy-Container
- Открываем атрибут defaultSecurityDescriptor, схраняем куда-нибудь его содержимое на всякий случай
- Добавляем в конец строки следующее: **(A;CI;LCRPLORC;;;DC)** Означает это следующее:

```
Примечание.
```

```
Тип доступа: A = Access Allowed
Флаг ACE: CI = Container Inherit
Разрешения:
LC = List Contents
RP = Read All Properties
LO = List Object
RC = Read Permissions
Субъект доступа: DC = Domain Computers
```

- Чтобы применить изменения, нужно перезагрузить схему. Для этого откройте mmc консоль и добавьте оснастку AD Schema (если оснастка отсутствует, зарегистрируйте библиотеку regsvr32 schmmgmt.dll и перезапустите mmc консоль). Щелкните ПКМ по Active Directory Schema и выберите Reload the Schema

microsoft, KB3163622, MS16-072, поломали, GPO