Finding Passwords in SYSVOL & Exploiting Group Policy Preferences

By Sean Metcalf

Published: 2015-12-28 · Archived: 2026-04-06 02:08:57 UTC

At Black Hat and DEF CON this year, I spoke about ways attackers go from Domain User to Domain Admin in modern enterprises.

Every Windows computer has a built-in Administrator account with an associated password. Changing this password is a security requirement in most organizations, though the method for doing so is not straight-forward. A standard method is to use Group Policy to set the local Administrator password across a large number of workstations. A major issue with this is that all of the computers have the same local Administrator password. Windows is extremely helpful when it comes to local accounts since if two (or more) computers have the same local account name and password, Windows will authenticate the account as if it is local, meaning that by gaining knowledge of the administrator credential on one system, the attacker can gain admin access to all of them (that have the same local administrator credentials).

SYSVOL

One of these methods is mining SYSVOL for credential data.

SYSVOL is the domain-wide share in Active Directory to which all authenticated users have read access. SYSVOL contains logon scripts, group policy data, and other domain-wide data which needs to be available anywhere there is a Domain Controller (since SYSVOL is automatically synchronized and shared among all Domain Controllers).

All domain Group Policies are stored here: \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\

Credentials in SYSVOL

A big challenge for administrators has been ensuring that the local Administrator account (RID 500) on all Windows computers. The traditional method for doing this (other than buying a product) has been to use a custom script to change the local administrator password. This issue with this is that frequently the password is stored in clear-text within the script (such as a vbs file) which is often in SYSVOL. Here’s an example of one of the top results when searching for a VBS script that changes the local Administrator password. The vbs script is still available on the Microsoft TechNet gallery and the password is obvious. Remember this script is stored in SYSVOL which every domain user has read access to and the password is the local Administrator password for every computer the Group Policy is applied to.

Changes the local Administrator password. The script should be deployed using Group Policy or through a logon script.

Visual Basic

```
Set oShell = CreateObject("WScript.Shell")
Const SUCCESS = 0

sUser = "administrator"
sPwd = "Password2"

' get the local computername with WScript.Network,
' or set sComputerName to a remote computer
Set oWshNet = CreateObject("WScript.Network")
sComputerName = oWshNet.ComputerName

Set oUser = GetObject("WinNT://" & sComputerName & "/" & sUser)

' Set the password
oUser.SetPassword sPwd
oUser.Setinfo

oShell.LogEvent SUCCESS, "Local Administrator password was changed!"
```

Please don't use this script to change the local Administrator password.

Group Policy Preferences

In 2006, Microsoft Bought Desktop Standard's "PolicyMaker" which they re-branded & released with Windows Server 2008 as "Group Policy Preferences." One of the most useful features of Group Policy Preferences (GPP) is the ability to store and use credentials in several scenarios. These include:

- Map drives (Drives.xml)
- Create Local Users
- Data Sources (DataSources.xml)
- Printer configuration (Printers.xml)
- Create/Update Services (Services.xml)
- **Scheduled Tasks (ScheduledTasks.xml)**
- **Change local Administrator passwords**

That's very helpful for administrators since it provides an automated mechanism for what previously required a custom solution such as a script. It provides useful capability to leverage Group Policy to "deploy" scheduled tasks with explicit credentials and change the local admin passwords on large numbers of computers at once – probably the two most popular usage scenario.

Credential Storage in Group Policy Preferences

The question at this point should be: how is the credential data protected?

When a new GPP is created, there's an associated XML file created in SYSVOL with the relevant configuration data and if there is a password provided, it is AES-256 bit encrypted which should be good enough…

Except at some point prior to 2012, Microsoft published the AES private key on MSDN which can be used to decrypt the password. Since authenticated users (any domain user or users in a trusted domain) have read access to SYSVOL, anyone in the domain can search the SYSVOL share for XML files containing "cpassword" which is the value that contains the AES encrypted password.

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-
    02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
    <Properties action="U" newName="ADSAdmin" fullName="" description=""
      cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ"
      changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
      (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```

Exploiting Group Policy Preferences

With access to this XML file, the attacker can use the AES private key to decrypt the GPP password. The PowerSploit function Get-GPPPassword is most useful for Group Policy Preference exploitation. The screenshot here shows a similar PowerShell function encrypting the GPP password from an XML file found in SYSVOL.

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ'
#Super@Secure&Password$2015?
```

Oddvar Moe notes a quick way to search for these:

```
findstr /S /I cpassword \\<FQDN>\sysvol\<FQDN>\policies\*.xml
```

From what I can find, the issues with GPP credentials was first written about by Emilien Gauralt in the post "Exploiting Windows 2008 Group Policy Preferences" in January 2012. Unfortunately the link is dead and the content offline. A few months later in May, Chris Campbell – wrote the article "GPP Password Retrieval with PowerShell" as well as the first PowerShell code to exploit this issue. Chris later updated the PowerShell code and added Get-GPPPassword to PowerSploit. About a month later, in June, "Rewt dance" posted a GPP exploitation expanded reference (link offline – google cached version). I also recently discovered Alexandre Herzog's post "Exploit credentials stored in Windows Group Policy Preferences" (dated April 2012).

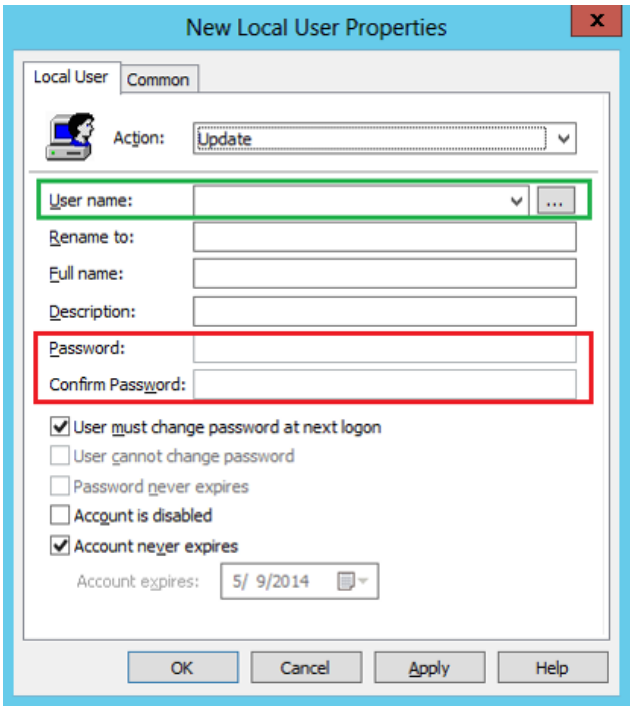
I have written about the problems with credentials in Group Policy Preferences and the GPP patch (KB2962486).

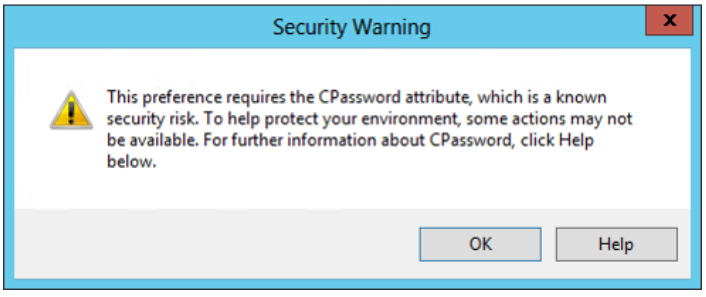
I continue to find administrative credentials (including Domain Admin credentials) in Group Policy Preference XML files in SYSVOL, especially for scheduled tasks running under the context of admin accounts.

The Group Policy Preference Credential Patch (KB2962486)

The obvious question for defenders is how to protect against this?

Microsoft released a patch in May 13, 2014 : "MS14-025 Vulnerability in GPP could allow elevation of privilege" (KB2962486). This patch needs to be installed on all systems that administer Group Policy using the Remote Server Administration Tools (RSAT). This patch prevents admins from putting password data into a Group Policy Preference.





Note that existing Group Policy Preference files with passwords are not removed from SYSVOL

Microsoft provides a sample PowerShell script for finding GPP passwords in SYSVOL: https://support.microsoft.com/en-us/help/2962486/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevation-of-privilege-may-13,-2014

Group Policy Preference Exploitation Detection:

XML Permission Denied Checks

- Place a new xml file in SYSVOL & set Everyone:Deny.
- Audit Access Denied errors.
- Sing the associated GPO doesn't exist, there's no legitimate reason for access.

Group Policy Preference Exploitation Mitigation:

- Install KB2962486 on every computer used to manage GPOs which prevents new credentials from being placed in Group Policy Preferences.
- Delete existing GPP xml files in SYSVOL containing passwords.

Microsoft Local Administrator Password Solution (LAPS)

The best Microsoft provided method for changing local Administrator passwords is the "Local Administrator Password Solution" aka LAPS.

References:

- Sean's presentation slides & videos on Active Directory security
- Group Policy Preferences AES private key on MSDN
- Using Group Policy Preferences for Password Management = Bad Idea
- GPP Password Retrieval with PowerShell
- The PowerSploit function Get-GPPPassword
- Group Policy Preferences Password Vulnerability Now Patched
- Microsoft Local Administrator Password Solution (LAPS)
