What is SYSVOL?

SYSVOL is a shared folder hosted on every Domain Controller that stores Group Policy and logon scripts, and every authenticated user can read it. The classic risk is Group Policy Preferences (GPP) passwords: administrators once stored credentials in GPP XML files in SYSVOL, encrypted with an AES key Microsoft publicly documented, so anyone in the domain could decrypt them. Even after the MS14-025 fix, legacy files often remain, making SYSVOL a fast, quiet credential win for attackers.

HOW IT WORKS

01 The GPP password leak and payload

The well-known abuse is GPP passwords. Administrators used Group Policy Preferences to set local-account passwords, which were stored in XML files (`Groups.xml` and similar) in SYSVOL, encrypted with AES, but Microsoft published the key. So any domain user could read and decrypt them.

- Find and decrypt automatically: `Get-GPPPassword` (PowerSploit) or `gpp-decrypt <cpassword>`
- Search SYSVOL for leftover secrets in scripts and XML.

Microsoft removed the feature in MS14-025, but pre-existing files were not deleted, so legacy `cpassword` values still surface. Shown for defensive context.

> STILL WORTH CHECKING
>
> *The MS14-025 patch stopped new GPP passwords but did not remove old ones. Search SYSVOL for* `cpassword` *and for credentials hard-coded in logon scripts, both common findings years later.*

HOW TO DEFEND

- Search SYSVOL for `cpassword` and remove any legacy GPP files containing it.
- Apply MS14-025 so new GPP passwords cannot be created.
- Remove credentials from logon scripts and other SYSVOL files; use proper secret management instead.
- Rotate any password ever stored in SYSVOL, assuming it is compromised.
- Audit SYSVOL access patterns for mass reads.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] NIST SP 800-115 Technical Guide to Security Testing

[3] Microsoft: Kerberos Authentication Overview

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-sysvol-gpp-passwords

Open online