2013-07-11
Xavier de Carné de Carnavalet

# WINDOWS 7/8 ADMIN ACCOUNT INSTALLATION PASSWORD STORED IN THE CLEAR IN LSA SECRETS

## BACKGROUND

"Windows LSA Secrets" are stored in an encrypted form in registry along with the respective encryption keys at HKEY_LOCAL_MACHINE\Security\Policy\Secrets which is not directly accessible by an admin account. SYSTEM permissions are required to browse this key, which can be achieved by installing any service, dumping the registry hives by booting another OS on the machine, or by getting any sort of quick admin access (unlocked computer).

Each secret contains a modification timestamp (Cupdtime), the current encrypted value (CurrVal), a security policy saying which user can access the secret (SecDesc), but it also stores the previous value of the secret (OldVal) and its modification timestamp (OupdTime). By using the standard Windows API, changing the value of a secret will automatically keep the previous value as OldVal.

When using autologin feature, the password for the autologged account is stored as the current value of *DefaultPassword* secret for Windows to use it instead of asking the password to the user.

## VULNERABILITY DESCRIPTION

*DefaultPassword* secret also stores the admin account password provided during Windows 7/8 installation.
During the first boot, the *DefaultPassword* current value contains the user password. After a reboot, the current value is overwritten with an empty value but the mechanism behind the LSA Secrets keeps the cached password as the old value which is still accessible until someone changes the secret.

Because the user is not prompted for his/her password at first boot, we believe the autologin feature is being used at that time and disabled right after, making the password cached in the LSA Secrets. Failure to properly erase the password used for autologin is believed to be the cause of the problem.

## PROOF OF CONCEPT

- Boot on a Windows 7/8 installation disk and proceed with installation
- Provide a password for the created admin account on "Set a password for your account" screen
- After being logged on to the desktop, reboot the computer
- With admin privileges or by booting on another device, dump the SYSTEM and SECURITY hives
- On any computer, launch ElcomSoft Proactive System Password Recovery, go to Advanced features > NT secrets, check Manual decryption, provide the dumped hives, check Show old secrets and press Manual decryption
- Two values of *DefaultPassword* are shown: the current one which is empty, and the old one, which contains the password provided at installation in plaintext

## VULNERABLE/TESTED VERSIONS

Checked on: Windows XP SP3 x86, Windows Vista SP2 x86 Business, Windows 7 SP1 x64 Home Premium/Pro, Windows 8 x64 Pro (MSDNAA ISOs)
Affected products: Windows 7, 8

On Windows XP, the password provided at installation is not cached. However, when an admin user changes his/her password when currently logged with his/her account using User Accounts in Control Panel, the changed password is cached as the current value of *DefaultPassword*. The previous password is still stored as the OldVal of the secret. Windows XP does not store the password when it is changed through net user or control userpasswords2. Non-admin passwords are not cached either.

Windows Vista doesn't seem to be affected by installation password nor password change plaintext caching. It is to be noted that a user needs to enter his/her password even on the first boot.

On Windows 8, only local accounts are vulnerable while online Microsoft accounts, created or already existing, are not subject to this plaintext caching. In addition, at the first boot, it is possible to see the *DefaultPassword's* OldVal which gets replaced at installation. While it is empty on Windows 7, the value is "ROOT#123" on Windows 8 (and Vista), which appears to be the default admin password on some beta builds.

## Real-world exploitation scenarios

A malicious user who gets a quick access to a system with admin privileges can retrieve an admin password in little time and later use this password, if it has not been changed since installation, for wider malicious purposes.

When using a company, school or public computer such as the ones provided for a short period loan, a malicious user has all the liberty to physically retrieve the needed registry files to get the admin password of the local machine and can then compromise all similar computers using the recovered password independently of its complexity.

## Vendor contact timeline

2013-05-20: Bug found
2013-06-14: Contacted Microsoft Security Response Center
2013-06-14: Reply from Microsoft SRC:
"the behavior you are reporting is not something that we consider a security vulnerability"
2013-07-11: Disclosure

## Workarounds/Limitations

- Do not setup a password during installation, or change it right after (recoverable password becomes useless).
- Store an empty value as *DefaultPassword* through LsaStorePrivateData() to flush the old value containing the password (requires admin privileges).
- During the first boot after installation of Windows, store twice an empty value to flush completely.
- Delete HKEY_LOCAL_MACHINE\Security\Policy\Secrets\DefaultPassword (requires SYSTEM privileges).
- Network installation for Windows 7/8 (SCCM) do not seem to be affected by the issue.

## References

http://seclists.org/fulldisclosure/2006/May/119
http://www.passcape.com/index.php?section=docsys&cmd=details&id=23