

Windows 8 stores logon passwords in plain-text

© 2012 Passcape Software
Passcape Software

1. Windows 8 stores logon passwords in plain-text	3
---	---

1 Windows 8 stores logon passwords in plain-text

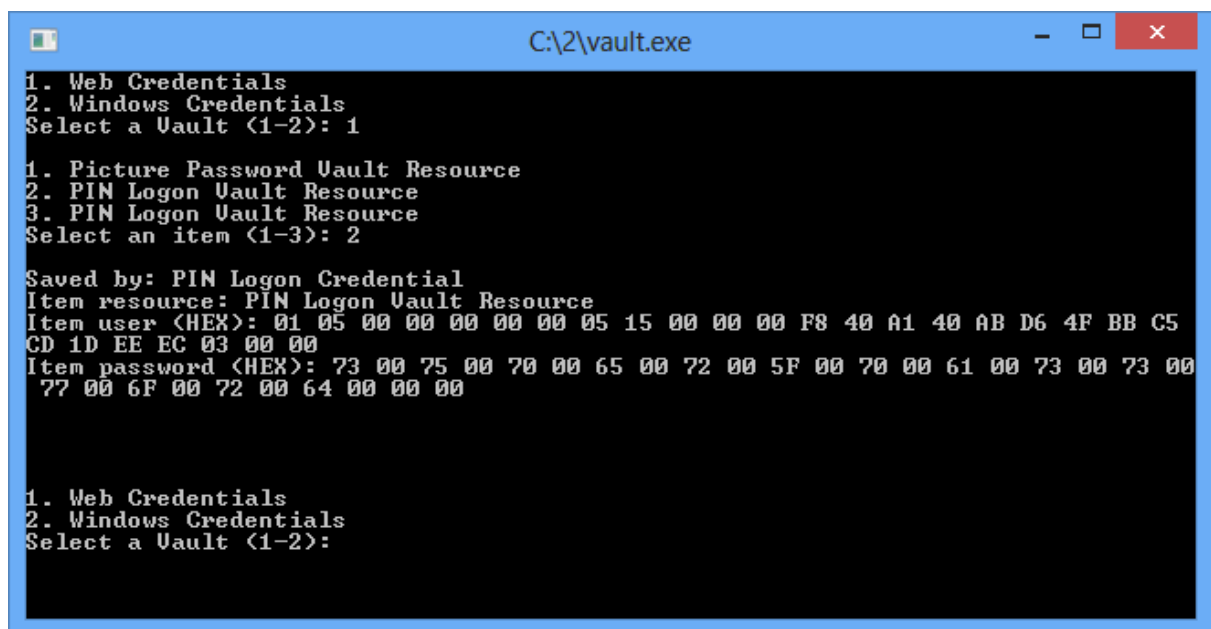
In one of our previous articles, you could read about [ways to recover text passwords in Windows](#) without brute-forcing them, locations in the system where text passwords could reside and tools used for the recovery. It turns out the release of Windows 8 is not without another fly in the ointment either. Our experts have discovered a serious flaw in the two new ways of logging on to the system. We are talking about [Picture password](#) and PIN.

The matter is that these two authentication methods are based on a regular user account. In other words, the user must first have created an account with a regular password and then optionally switch to PIN or picture password authentication. Notably that the original plain-text (!) password to the account also remains in the system.

Once the user has switched to a new authentication method, his text password is encrypted using the **AES** algorithm and saved to protected Vault storage in the following folder:

```
%SYSTEM_DIR%/config/systemprofile/AppData/Local/Microsoft/Vault/4BF4C442-9B8A-41A0-B380-DD4A704DDB28
```

This system folder contains **Vault** records with SIDs and text passwords of all users with active PIN or picture password authentication. The text password is not bound to the PIN or picture password; therefore, any user of the PC with the Administrator privileges can easily recover it (the encryption key is protected with system [DPAPI](#)).



```
C:\2\vault.exe
1. Web Credentials
2. Windows Credentials
Select a Vault <1-2>: 1

1. Picture Password Vault Resource
2. PIN Logon Vault Resource
3. PIN Logon Vault Resource
Select an item <1-3>: 2

Saved by: PIN Logon Credential
Item resource: PIN Logon Vault Resource
Item user <HEX>: 01 05 00 00 00 00 00 05 15 00 00 00 F8 40 A1 40 AB D6 4F BB C5
CD 1D EE EC 03 00 00
Item password <HEX>: 73 00 75 00 70 00 65 00 72 00 5F 00 70 00 61 00 73 00 73 00
77 00 6F 00 72 00 64 00 00 00

1. Web Credentials
2. Windows Credentials
Select a Vault <1-2>:
```

Pic. 1. Decrypting passwords for all users with active PIN or picture password authentication.

Briefly, Vault can be described as a protected storage for user's private data. Windows Vault emerged with the release of Windows 7 and could store various network passwords. In Windows 8, Vault has extended its functionality; it has become a more universal storage but at the same time lost its compatibility with the previous versions. Thus, the 'old' Vault implements a custom password protection. While in Windows 8, it seems, this feature is

frozen and it uses DPAPI-based protection only. Windows Vault is used by other applications as well. For example, Internet Explorer 10 uses it to store passwords to websites.

Some of our [password recovery utilities](#) already implement Windows 8 plain-text password decryption. The upcoming release of Windows Password Recovery is expected to have a full-fledged Vault analyzer and offline decoder.

Picture password and PIN are completely new authentication methods in Windows 8, an attempt to escape from the password-remembering hell. However, use them with caution. If an account is configured for authentication using picture password or PIN, your original plain-text password is stored in the system, and any user with the Administrator privileges can gain access to it.