Author(s): **Ivan Sanchez**
Contact Us: **ivan.sanchez@nullcode.com.ar**
Date: 27/07/2014
Product: dtSearch Corp
Vendor: Notified

We have discovered that some products from dtSearch Corp, presents a big hole regarding a DLL hijacking. The basis of this exploit is the way in which dtseach product works and how it loads DLL files used by many applications, if an application calls a DLL without specifying an absolute path Windows will conduct a search for the DLL file in various set locations.

BINARY PLANTING
DLL HIJACKING
DLL PRELOADING
UNSAFE LIBRARY LOADING

Product installed to audit the code:

Application: DtImage.exe
Version: 7, 0, 0, 1
Product Name: dtSearch Desktop
Description: Image Viewer
Application Path: C:\Program Files\dtSearch\bin\dtImage.exe

Case 1) File Affected Untrusted Library Loading Execution Code:

Application: dtImage.exe

DLL Affected:

imhost32.dll

Vector Attack:

Real world examples:

1. Attacker sends a shared folder link to a victim. Victim opens and sees some .html files and double-clicks one of them. When a vulnerable browser or application opens this file it loads a dll directly from this share, and victim is now infected.
2. Attacker posts a link in a forum that looks like a http link but redirects victim to a shared folder. Victim opens a simple .pdf file and gets infected.
3. Attacker gains access to a trusty website and puts iframes or redirects to his share. Victim trusts this site and opens an mp3 file inside the shared folder and… gets infected as well.
4. Attacker uses the .lnk bug or any browser vulnerability together with any of above examples and thus increase his infect rate.

http://www.offensive-security.com/offsec/microsoft-dll-hijacking-exploit-in-action/

\\Internet -Share\\ dtImage.exe + DLLs affected   (EVIL DLL)

(Dll affected will execute the evil code when the end user open /run the APP)

Thanks in advance   (Ivan)

www.nullcode.com.ar   www.evilcode.com.ar

Nullcode & Evilcode Team