Advisory Name: Windows Script Host DLL Hijacking

Internal Cybsec Advisory Id: 2011-0901-Windows Script Host DLL Hijacking

Vulnerability Class: Remote Command Execution Vulnerability

Release Date: September 2, 2011

Affected Applications: Windows Script Host v5.6; other versions may also be affected

Affected Platforms: Any running Windows Script Host v5.6

Local / Remote: Remote / Local

Severity: High – CVSS: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

Researcher: Juan Manuel Garcia

Vendor Status: Acknowedged

Reference to Vulnerability Disclosure Policy: http://www.cybsec.com/vulnerability_policy.pdf

Vulnerability Description:

DLL Hijacking takes advantage of the way an application dynamically loads dll libraries without specifying a fully qualified path. This is usually done invoking the LoadLibrary and LoadLibraryEx functions to dynamically load DLLs.

In order to exploit this vulnerability a user must open a file with an extension associated to the vulnerable application. A malicious dll, named exactly as a dll the apllications loads using the vulnerable function, must be placed in the same directory as the opened file. The application will then load the malicious dll instead of the original, thus executing the malicious code.

The following application loads external libraries following an insufficiently qualified path.

- Application: wscript.exe
- Extensions: js, jse, vbe, vbs, wsf, wsh
- Library: wshesn.dll

Exploit:

- Option 1 - Using the “msfpayload” Metasploit module as shown below:

msfpayload windows/exec CMD=calc.exe D > exploit.dll

- Option 2 - Using the “webdav_dll_hijacker” Metasploit module.

Impact:

A successful exploit of this vulnerability leads to arbitrary code execution.

Vendor Response:

2011/08/09 – Vulnerability was identified.
2011/08/19 – Cybsec sent detailed information on the issue and a Proof of Concept.
2011/08/19 – Vendor stated: “As a matter of policy, we cannot comment on ongoing investigations”.
2011/08/19 – Vendor was informed that the security advisory would be published after 15 days.
2011/09/02 – Vulnerability was released.

Contact Information:

For more information regarding the vulnerability feel free to contact the researcher at
jmgarcia <at> cybsec <dot> com

About CYBSEC S.A. Security Systems

Since 1996, **CYBSEC** is engaged exclusively in rendering professional services specialized in Information Security. Their area of services covers Latin America, Spain and over 250 customers are a proof of their professional life.

To keep objectivity, CYBSEC S.A. does not represent, neither sell, nor is associated with other software and/or hardware provider companies.

Our services are strictly focused on Information Security, protecting our clients from emerging security threats, maintaining their IT deployments available, safe, and reliable.

Beyond professional services, CYBSEC is continuously researching new defense and attack techniques and contributing with the security community with high quality information exchange.

For more information, please visit www.cybsec.com