



COT Security Alert – DLL Load Hijacking

The Security Administration Branch has become aware of an exploit of a known Microsoft Windows application vulnerability involving the way dynamically linked libraries (DLL) are loaded and called. Dynamic-Link Libraries are executable files that act as a shared library of functions and provide a way for an application to call a function that is not part of its own executable code. An attacker may place a malicious DLL named as a legitimate DLL in the current working directory, thereby enabling the attacker-supplied DLL to be called by an application rather than the legitimate DLL. This then results in the execution of the arbitrary code in the attacker-supplied DLL. In order for an exploit to be successful, the DLL file must be located on a WebDAV, SMB, extracted archive or a USB key share.

While this is a Microsoft vulnerability, it involves multiple third-party software vendors. Each affected vendor must supply a product update in order for its application to be patched against this vulnerability.

References and Additional Information:

Microsoft:

<http://blogs.technet.com/b/srd/archive/2010/08/23/more-information-about-dll-preloading-remote-attack-vector.aspx>

<http://blogs.technet.com/b/msrc/archive/2010/08/21/microsoft-security-advisory-2269637-released.aspx>

<http://www.microsoft.com/technet/security/advisory/2269637.mspx>

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
<http://technology.ky.gov/ciso/>