

Next Generation Network Access Technology

Insecure Library Loading Vulnerability

NCP's Secure Client products had been vulnerable to a Dynamic-Link Library (DLL) hijacking attack that exploits a weakness when applications load external libraries in Microsoft Windows. If an application loads a DLL using the function LoadLibrary(ex) without a fully qualified path, it searches for missing DLLs in the following order:

1. The directory from which the application loaded (installation directory)
2. The system directory
3. The 16-bit system directory
4. The Windows directory
5. The current working directory
6. The directories that are listed in the PATH environment variable

This way a malware-infested DLL file that is located in the working directory of the client monitor could be loaded with the access rights of the user starting the program. All NCP DLL files that are located in the client installation directory are not affected by this. However, there is a potential risk for external DLLs that are checked for their availability by the client. If a VPN configuration file is opened from a network drive by double clicking on it, a malware infested DLL is located in the same place and the client monitor is currently not loaded, the infested DLL is loaded and malicious code could be executed.

NCP Secure Client Updates

Patches to eliminate this vulnerability are included in the following versions of the NCP Secure Client:

- NCP Secure Enterprise Client (Win 32/64) 9.21 Build 68 (or secureVPN)
- NCP Secure Entry Client (Win 32/64) 9.23 Build 18
- NCP Secure Client - Juniper Edition: 9.23 Build 18

Download: <http://www.ncp-e.com/en/downloads/software.html>

The versions listed above have been fixed to ignore the working directory for loading DLLs. Users must have Microsoft Windows XP (SP1 and later), Windows Vista or Windows 7.

Our support team is happy to answer any questions you might have. Please do not hesitate to contact us at helpdesk@ncp-e.com.