Example of research paper on windows operating system vulnerabilities

Business, Company

Windows Operating System Vulnerabilities

Windows 7, the latest version of the operating system released by the Microsoft Company, is built on the enhanced security platform of Windows Vista, thus including approach called defense-in-depth. According to one of the Windows team members, Paul Cooke, it is aimed at customers' protection from malware and is based on such features as Kernel Patch Protection, User Account Control (UAC), Windows Service Hardening and others (2009). Development and improvement of these technologies made the system the most secure among the Windows operating systems.

Still, this system, as any other ones, has its own vulnerabilities discovered as a result of some independent tests (Windows 7 Security Vulnerabilities, n. d.; Wisniewski, 2009). In this paper I will describe the ones that are the most dangerous for the PC security. The first of them possesses CVSS score of 9. 3 and has complete impact on confidentiality, integrity and availability of the system. It is a stack-based buffer overflow in the CFrameWnd class in UpdateFrameTitleForDocument method in mfc42. dll in the Microsoft Foundation Class (MFC) Library (CVE-2010-3227, 2010). It allows context-dependent attackers execute arbitrary codes through long window titles.

Another Windows 7 vulnerability, possessing the same CVSS score of 9. 3 represents untrusted search path in wab. exe 6. 00. 2900. 5512 in Windows Address Book. It allows users to make use of a Trojan horse wab32res. dll file in the active working directory (CVE-2010-3147, 2010). The last Windows 7 vulnerability I am going to explore is one having 7. 6 CVSS score and allowing for major security threats to the system. It is heap-based overflow in Microsoft Windows Fax Services Cover Page Editor 5. 2 r2 in fxscover. exe in

the CDrawPoly:: Serialize function (CVE-2010-4701, 2011). It provides a chance to remote attackers to execute arbitrary codes through long record in the Fax Cover Page (. cov) file.

Thus, although Windows 7 is the most secure among the other Windows operating systems, it doesn’t mean that it can fully protect computer from all kinds of threats (Ragan, 2011). It is still necessary to have and run quality antivirus to keep information and system secure.

References

Cooke, P. (2009, November 6). Windows 7 Vulnerability Claims [blog]. Retrieved from http://windowsteamblog. com/windows/b/windowssecurity/archive/2009/11/06/windows-7-vulnerability-claims. aspx

Microsoft Windows 7 Security Vulnerabilities. (n. d.). Retrieved from http://www. cvedetails. com/vulnerability-list/vendor_id-26/product_id-17153/hasexp-1/Microsoft-Windows-7. html

Ragan, S. (2011, February 16). RSAC 2011: Windows 7 vulnerabilities show need for kernel control [blog]. Retrieved from http://www. thetechherald. com/article. php/201107/6830/RSAC-2011-Windows-7-vulnerabilities-show-need-for-kernel-control

Vulnerability Details: CVE-2010-3147. (2010). Retrieved from http://www. cvedetails. com/cve/CVE-2010-3147/

Vulnerability Details: CVE-2010-3227. (2010). Retrieved from http://www. cvedetails. com/cve/CVE-2010-3227/

Vulnerability Details: CVE-2010-4701. (2011). Retrieved from http://www.

cvedetails. com/cve/CVE-2010-4701/

Wisniewski, C. (2009, November 3). Windows 7 vulnerable to 8 out of 10 viruses [blog]. Retrieved from http://nakedsecurity. sophos. com/2009/11/03/windows-7-vulnerable-8-10-viruses/

References