February 2008

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

FEDERAL DESKTOP CORE CONFIGURATION (FDCC): IMPROVING SECURITY FOR WINDOWS DESKTOP OPERATING SYSTEMS

Shirley Radack and Karen Scarfone, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The Federal Desktop Core Configuration (FDCC) is a standard security configuration mandated by the Office of Management and Budget (OMB). The FDCC currently exists for the Microsoft Windows XP Professional™ and Windows Vista Enterprise™ operating systems. In March 2007, OMB issued policy guidance in a memorandum to all federal agencies and departments requiring that they develop plans to adopt the standard security configuration for their Windows XP Professional (using Service Pack 2) and Vista Enterprise-based systems by February 1, 2008. The goal of the FDCC is to help federal organizations improve their information security and reduce the information technology (IT) costs associated with securing their Windows operating systems.

The FDCC was created by customizing existing security recommendations for Windows and Internet Explorer 7.0. Specifically, the Windows XP FDCC was based on Air Force customization of the Specialized Security-Limited Functionality (SSLF) recommendations in NIST Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, and Department of Defense (DoD) customization of the recommendations in the Microsoft Security Guide for Internet Explorer 7.0. The Windows Vista FDCC was based on DoD customization of the Microsoft Security Guides for Windows Vista and Internet Explorer 7.0. Microsoft's guide for Vista was produced through a collaborative effort with the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the Information Technology Laboratory of the National Institute of Standards and Technology (NIST).

NIST provides several types of resources to help agencies understand and implement FDCC. The NIST FDCC website, located at http://fdcc.nist.gov/, provides information such as answers to frequently asked questions about the FDCC, workshop and conference presentations, FDCC settings documentation, and FDCC-related content and tools. Also, technical questions on FDCC that are not answered on the NIST FDCC website can be directed via email to a support capability at fdcc@nist.gov.

Testing FDCC Settings

Before deploying FDCC in an operational environment, agencies should thoroughly test certain FDCC settings that may impact system functionality. Examples of these are running the system as a standard user, requiring the use of Federal Information Processing Standard

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since January 2007:

- *Security Controls for Information Systems: Revised Guidelines Issued by NIST, January 2007*
- *Intrusion Detection and Prevention Systems, February 2007*
- *Improving the Security of Electronic Mail: Updated Guidelines Issued by NIST, March 2007*
- *Securing Wireless Networks, April 2007*
- *Securing Radio Frequency Identification (RFID) Systems, May 2007*
- *Forensic Techniques for Cell Phones, June 2007*
- *Border Gateway Protocol Security, July 2007*
- *Secure Web Services, August 2007*
- *The Common Vulnerability Scoring System, October 2007*
- *Using Storage Encryption Technologies to Protect End User Devices, November 2007*
- *Securing External Computers and Other Devices Used by Teleworkers, December 2007*
- *Secure Web Servers: Protecting Web Sites that are Accessed by the Public, January 2008*

(FIPS) 140-2 approved encryption, and installing drivers that are not digitally signed by Microsoft. Additional information on potentially problematic settings is available from NIST's FDCC web page, which is located at http://fdcc.nist.gov/.

Resources are available to agencies to assist them in performing FDCC-related testing. Microsoft has a product called Virtual PC (VPC) that allows users to run a virtual instance of an operating system (OS) within an already-running instance of an OS. The virtual instance, also known as a virtual machine, can utilize the hardware of the computer (e.g., hard drive, Ethernet card, Universal Serial Bus [USB] ports) in the same way the non-virtual OS does. From the non-virtual OS, the virtual machine appears as a single, large *.vhd file.

Virtual machines are useful for both laboratory and deployment testing. While software can be installed on a virtual machine in the same way software is installed on normal OSs, virtual machines can be discarded and reimplemented quickly for the purposes of ensuring a pristine testing environment or if something malfunctioned with the previous virtual machine. Additionally, multiple virtual machines can be run on a single physical platform to achieve cost savings.

Microsoft produces virtual machine *.vhd files for FDCC with input from many federal departments and agencies, including DHS, DISA, OMB, NIST, NSA, and USAF. These files are published quarterly and can be downloaded from http://fdcc.nist.gov/download_fdcc.html. Organizations should use these virtual machine files in test and evaluation environments only; they are not to be used as deployment images. It is also recommended that before running an FDCC virtual machine, that antivirus software be installed and configured and that the VPC networking be set to "Local only" or "Not connected" to help isolate the virtual machine.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

Deploying FDCC Settings

For most organizations, the recommended deployment method for FDCC is to implement the majority of FDCC settings using group policies as managed with Microsoft Group Policy Objects (GPO). Approximately 98 percent of all FDCC settings may be implemented through GPOs. The remaining security settings, such as the granular audit policy settings for Windows Vista, must be implemented locally through *.inf, batch, or manual methods. Small organizations may choose to implement the FDCC settings through local methods only.

Organizations that manage several operating systems through a Group Policy Management Console (GPMC) can apply GPOs with FDCC settings to specific Windows operating systems using a Windows Management Instrumentation (WMI) filter (WMI filtering is only recognized on Windows Vista, Windows XP, and Windows Server 2003). More specifically, create a WMI filter that selects applicable operating systems, and link that filter to the GPO applicable for those operating systems. If computers with Windows 2000 or previous Windows operating systems are present within the enterprise, these computers must be granted exception from the group policy using the Deny Read and Deny Apply Group Policy settings. Additional information is available at http://nvd.nist.gov/chklst_detail.cfm?config_id=88 and http://support.microsoft.com/kb/555253.

Using The Security Content Automation Protocol (SCAP) for FDCC

Another NIST effort that helps to support FDCC is the Security Content Automation Protocol (SCAP). SCAP is a protocol established by NIST that encompasses a suite of interoperable and automatable standardized security components. Because SCAP uses Extensible Markup Language (XML)-based components, SCAP is simultaneously machine and human-readable. SCAP enables security tools to automatically perform configuration checks on Windows computers, ensuring that they maintain the proper security settings throughout the systems life cycle. To meet the goals set forth in OMB Memorandum M-07-18, security configuration scanning tools that can use official SCAP content are needed. In support of this, NIST has established an SCAP Validation Program through the NIST National Voluntary Laboratory Accreditation Program (NVLAP), so that independent laboratories can be accredited to perform the testing necessary to validate that security tools can accurately parse the SCAP content required for their specific functionality. So far, three laboratories have been accredited for SCAP Validation and three IT security products have been certified for the SCAP "FDCC Scanner" Capability. Additional details on SCAP compliance are available at http://scap.nist.gov/.

FDCC baselines for Windows XP and Vista are available in SCAP format at http://fdcc.nist.gov/download_fdcc.html. Through the use of SCAP-compliant tools and the official FDCC SCAP content, agencies can routinely monitor their systems to ensure that the FDCC settings have not been altered as the result of patches, new software installation, or human interaction. The tools compare the deployed configuration against the official FDCC SCAP content and report on any discrepancies so that corrective action can be taken. (Some tools also have an automatic remediation capability.) A small number of FDCC settings cannot be verified with SCAP at this time; a list of these settings is available from the main FDCC website, http://fdcc.nist.gov/.

Agencies can use FDCC SCAP content to automate some of their documentation of technical security controls' compliance with the requirements of the Federal Information Security Management Act (FISMA). The FDCC SCAP content has FISMA compliance mappings embedded within it, so that SCAP tools can automatically generate NIST Special Publication (SP) 800-53 assessment and compliance evidence. Each low-level security configuration check is mapped to the appropriate high-level NIST SP 800-53 security controls. As NIST SP 800-53A is finalized, there will be direct linkages, where appropriate, of the assessment procedures from SP 800-53A to the SCAP automated testing of information system mechanisms and associated security configuration settings. In addition, the FDCC SCAP content also contains mappings to other high-level policies, such as DoD 8500 and the Federal Information System Controls Audit Manual (FISCAM), and SCAP tools may also output those compliance mappings.

Reporting on FDCC Compliance

Per the July 31, 2007, memorandum from OMB to federal CIOs, federal agencies must use SCAP-validated products to verify that their Windows XP Professional and Vista Enterprise systems are FDCC-compliant. As an integral part of the continuous monitoring of systems configured to FDCC, agencies can report their testing results to NIST. To ensure both the accuracy and consistency of these results, agencies can use the standardized SCAP XML reporting format. Use of this format will enable NIST to efficiently collect and organize the results for analysis and trending over time. NIST will aggregate the results from all agencies, and will not generally provide direct feedback to each individual agency concerning their results.

OMB policy recognizes that agencies may determine that settings in the FDCC are not practical. In the March 20, 2007, memorandum to federal agency Chief Information Officers (see http://www.cio.gov/documents/Windows_Common_Security_Configurations.doc), OMB instructed agencies to provide documentation to NIST of any deviations from the FDCC and the rationale for doing so. Agencies are to report FDCC compliance through their CIO hierarchy; an agency or department CIO must report compliance for that organization. Compliance is expressed in a roll-up numbers of compliant versus noncompliant computers. For noncompliant computers, CIOs must provide a representative sample of SCAP-based assessment reports, using the Extensible Configuration Checklist Description Format (XCCDF) version 1.1.4. The FDCC XML reporting format is located at http://nvd.nist.gov/scap/content/fdcc-reporting_20080108.zip. Additional guidance will be forthcoming. This information should be sent to OMB at fisma@omb.eop.gov with a carbon copy to NIST at fdcc@nist.gov by March 31, 2008. NIST will perform trend analysis on all federal data and present findings to OMB.

For More Information

The Office of Management and Budget memoranda concerning the implementation of the FDCC, listed below, are available at: http://www.whitehouse.gov/omb/memoranda/

OMB Memorandum M-07-11 for the Heads of Department and Agencies; Implementation of Commonly Accepted Security Configurations for Windows Operating Systems, March 22, 2007

OMB Memorandum M-07-18 to Chief Information Officers and Chief Acquisition Officers; Ensuring New Acquisitions Include Common Security Configurations, June 1, 2007

OMB Memorandum for Chief Information Officers; Establishment of Windows XP and Vista Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations, July 31, 2007. See http://www.cio.gov/documents/FDCC_memo.pdf.

Additional information about FDCC is available on NIST's web page: http://fdcc.nist.gov/

For information about NIST standards and guidelines that are referenced in this bulletin, as well as other security-related publications, see http://csrc.nist.gov/publications/index.html.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.