Report Number: I743-010R-2006

NSA Windows Server 2003 Security Guide Addendum

Operational Network Vulnerability Office

Updated: Sept. 12, 2006
Version: 1.0

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

XPGuides@nsa.gov

Background

As part of a change in our development strategy for security guidance, the National Security Agency does not intend to publish a separate security guide for Windows Server 2003 beyond what was produced as a cooperative effort between the vendor and the security community. The "Specialized Security – Limited Functionality" (SSLF) security settings in Microsoft's "Windows Server 2003 Security Guide" track closely with the security level historically represented in the NSA guidelines. It is our belief that this guide establishes the latest best practices for securing the product and recommend that traditional customers of our security recommendations use the Microsoft guide when securing Windows Server 2003.

A Note on File and Registry Permissions:

Past NSA Windows guides recommended many changes to file and registry permissions. Typically, these changes were similar to the default operating system permissions, with the exception of the Everyone and Power Users or Server Operators groups being removed from the access control lists (ACLs).

However, NSA now believes that for Windows Server 2003, the default file and registry ACLs are generally sufficient given the following assumptions:

- Within Group Policy or Local Security Policy, the **"Network access: Let Everyone permissions apply to anonymous users"** security option is set to be **Disabled**.

The Microsoft Windows Server 2003 guide's discussion on "Securing the File System," lists optional security permissions for executables located primarily within the %SystemRoot%\system32 directory, stating that these permissions should be set only if the above-mentioned option is not configured. However, **NSA recommends setting these permissions regardless.**