SUBJECT: Installation of software/malware by unauthorized users.
AFFECTED SYSTEMS: Windows NT, 2000, 2000 Server, XP, 20003 Server.
THREAT LEVEL: 2/10
REMOTE OR LOCAL: Local Access Required.
PREVENTABLE: No.
WORKAROUND: None.

Brief Summary:

Vulnerability W031206101 can allow unauthorized users to gain complete control of an operating system. It allows a users to install almost any software that does not require extensive changes to, or access to restricted portions of the registry. By using this vulnerability, restricted users can install keyloggers, spyware, Trojans, or other malware; but cannot set them to run on system boot. However, the nature of such programs is that once activated they remain in the memory space even after logoff, and hence pose a security risk to all users of that particular computer.

Modus Operandi:

The X:\Documents and Settings\%Username%\ folder was meant as a local storage for any user. However, there exists a problem in that this is an obscure folder, quite often unlooked. It is used by windows as a place to store profile-related information and/or records for each user.

While it may be true that with local access to a PC, nothing is secure, this problem in particular poses a major security risk since it requires users to do nothing more than to point an installer to this folder, and in all likelihood, the installation will succeed.

The problem exists in that there is no way to specify what can or cannot be stored in this folder. Although it is true that the same can be done to the My Documents folder, users open that folder daily, and any new files might ring a bell. By contrast, most users will never open the \Documents and Settings\%Username%\ folder.

Analysis and Classification:

This is not a true security vulnerability, rather a loophole in the design of the kernel. The nature of Access Control Lists (ACL) is such that they offer protection by location, not by type. For instance, an administrator locks off access to certain folders with an ACL, and Windows ships with ACLs in place that prohibit users from modifying sections of the registry. At the same time, it does not prohibit certain *types* of files from running, and therein lies the hole that can be taken to a restricted users advantage.

End users can use this directory to install both harmless and harmful programs without resorting to using the folders on the Desktop and in the My Documents folder as install directories. In essence, this vulnerability makes the read-only restrictions on the Program Files directory a meaningless obstacle, but does not pose a security risk for other users of the computer.

Prevention:

This vulnerability's arguable threat level and "by-design" nature make it almost impossible to prevent, nevertheless, log-off filters set to delete executable files in such directories can achieve some sort of counter-measure, but nothing more.

Workarounds:

There is no known workaround, or no workaround is required.