Media Max Access Control Vulnerability

November 29th, 2005
Version 1.0

Confidential

Prepared by:
Jesse Burns and Alex Stamos of Information Security Partners LLC

Tested Product Version:
SunnComm Media Max 5.0.21.0 as installed from
My Morning Jacket: Z, and Sara McLachlan Bloom Remix Album
Other versions of Media Max have not been tested.

Platform verified on:
Complete verification on Microsoft Windows XP Service Pack 2
Weak ACL creation behavior also verified on Windows 2000

Description:

SunnComm Media Max version 5.0.21.0 (hereafter called Media Max), partially installs itself automatically the first time an affected CD is inserted into a Windows machine[1]. The automated installation includes the creation of a "SunnComm Shared" directory. Media Max creates this directory with a custom access control list[2] (ACL) that contains an access control entry (ACE) granting the Windows principal Everyone "Full Control" rights to the directory. This allows any process, user, or network client the ability to read, modify, and delete the contents of this directory, including low rights accounts which are not even members of the "Users" group. Granting untrusted users "Full Control" rights to executables that will be automatically run by high rights users creates a simple but serious security vulnerability[3].

[1] The automated installation is only partial as the user is eventually prompted with a EULA dialog box, at which point they can terminate the remainder of the installation. The partial installation remains however, including the weak ACL on the SunnComm Shared directory.

[2] An introduction to proper Windows Access Control Lists is available in Chapter 6 of *Writing Secure Code, 2nd Edition*, by Michael Howard and David LeBlanc, Microsoft Press

[3] This issue is also outlined in the Microsoft TechNet Security Management Column – "How to Shoot Yourself in the Foot with Security, Part 2: To ACL or Not to ACL"
http://www.microsoft.com/technet/community/columns/secmgmt/default.mspx

Here are some screen captures showing the file permissions of Media Max's main installation directory and the directory above it. The "Common Files" directory was created by Microsoft to be securely shared by multiple applications.

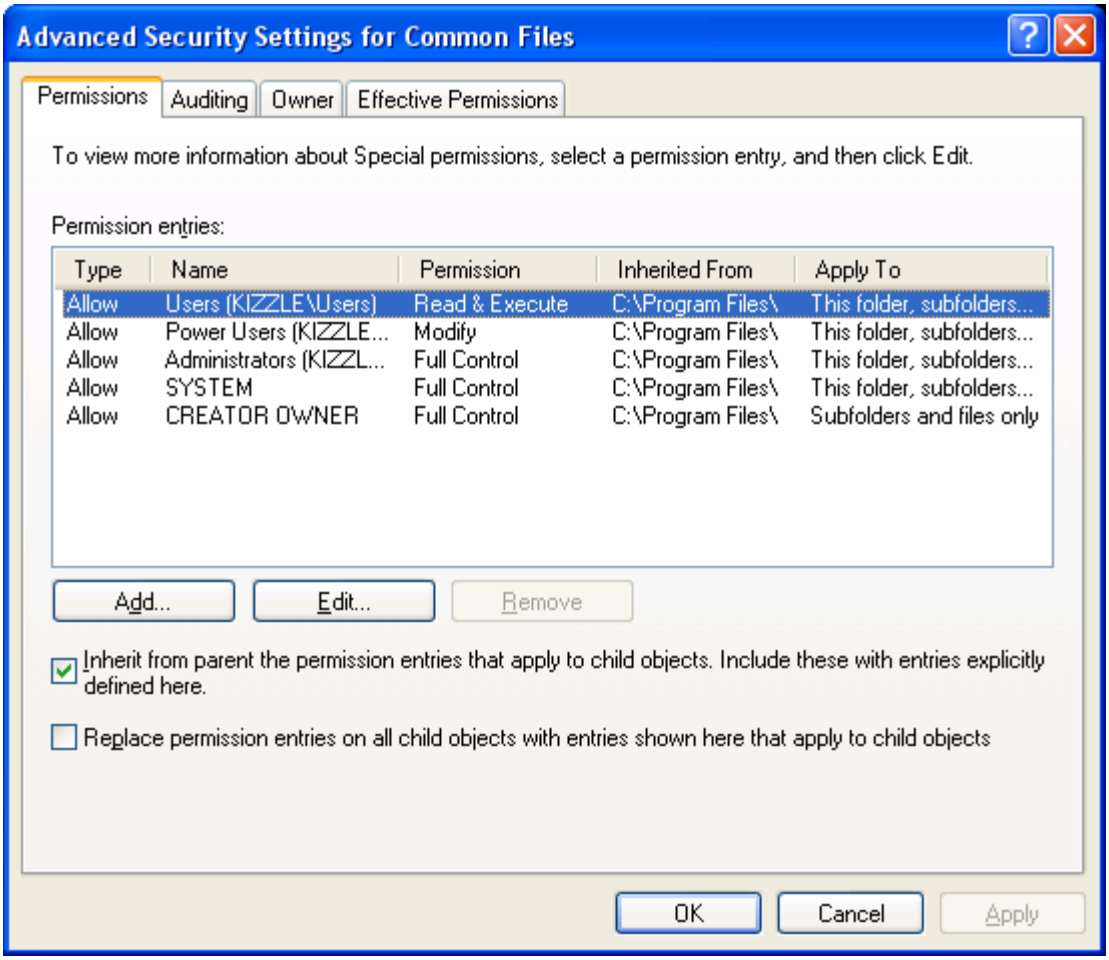

Figure 1: The security settings tab for C:\Program Files\Common Files

Note that the default "Common Files" ACL grants no rights to the Everyone principal and grants only read and execute rights to "Users" of the system. This allows for low rights users to access the software in this directory without granting them the ability to change or delete it.

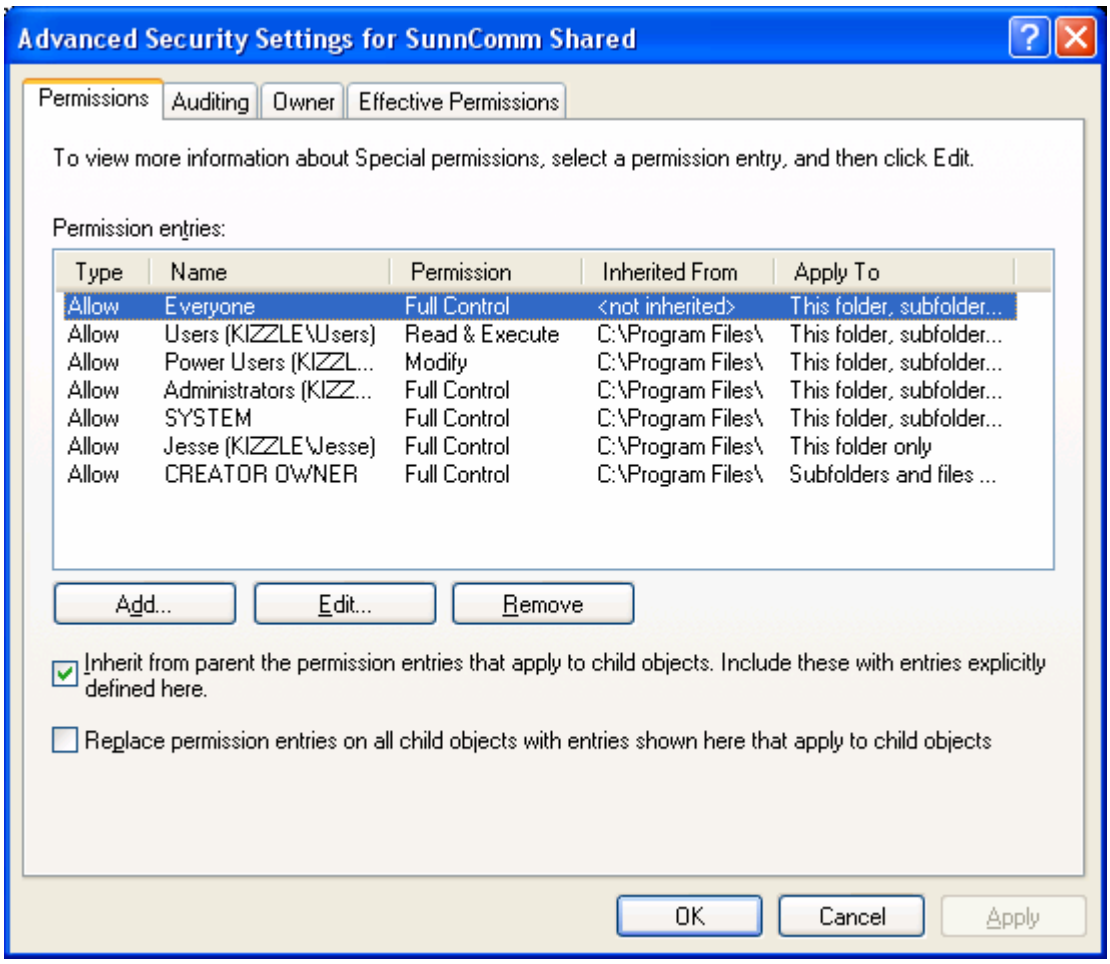

Figure 2: The security settings tab for C:\Program Files\Common Files\SunnComm Shared

Note the addition of the Everyone, Full Control, Access Control Entry.

After installation completes the "SunnComm Common" directory contains executable content like MMX.EXE, which runs automatically when a Media Max CD is inserted. The MMX.EXE program inherits the weak security protections configured by Media Max on the SunnComm Shared directory.

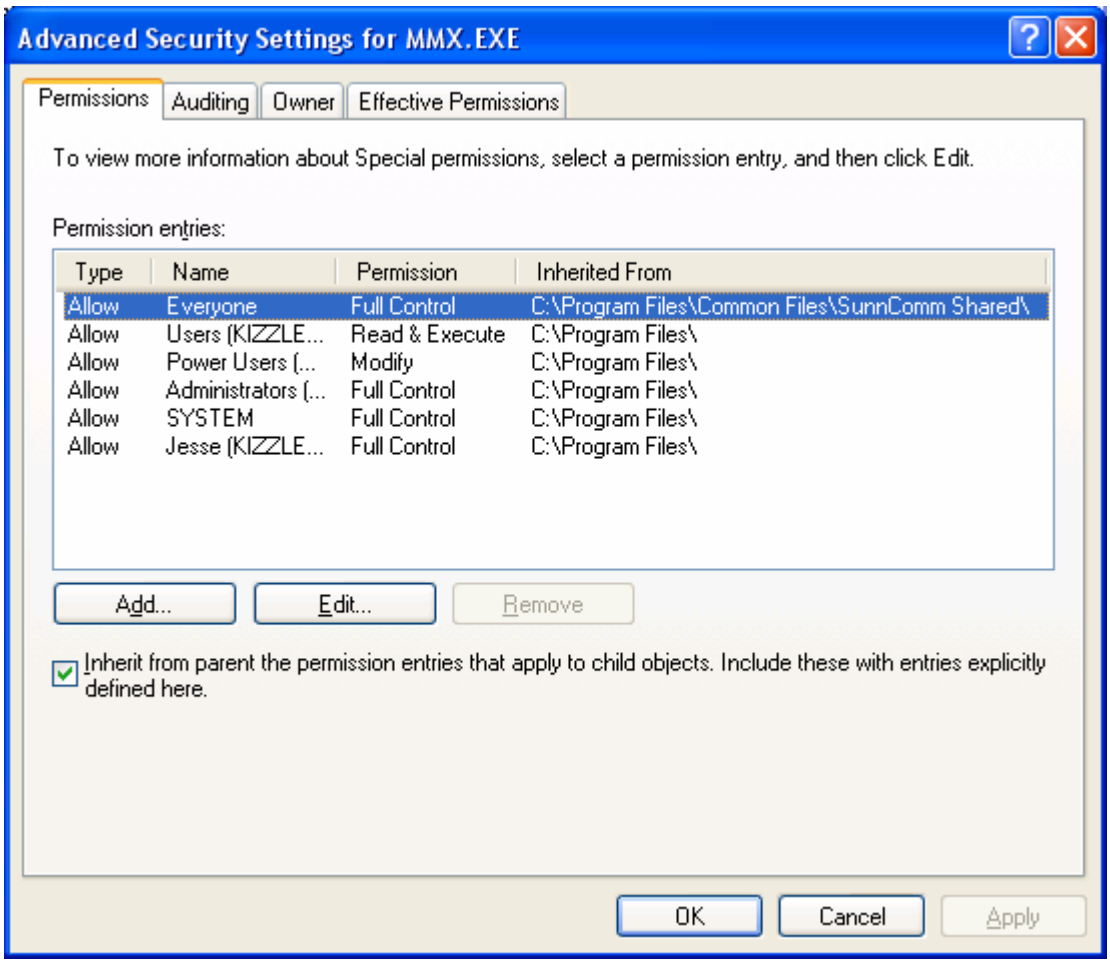

Figure 3: The security settings for MMX.exe showing it inheriting from SunnComm Shared

This ACE allows a low rights user to overwrite the file with hostile code. Other files in the directory share this same weakness which is inherited from the "SunnComm Shared" directory.

Correcting the file permissions using the Microsoft tools shown in figures 1, 2 and 3 is not effective as the next time a Media Max CD is played Media Max re-inserts the Everyone Full Control ACE into the ACL, thereby re-opening the vulnerability.

Exploit Scenario:

A machine with Media Max installed upon it is being used by a user with low rights. This access could be remote, through Windows file sharing, or local by use of the "guest" or another low rights account. The user either decides to attack the vulnerable system themselves or exposes the machine to malicious code inadvertently (for example by running an email virus). The attacker replaces the MMX.exe program that is installed by Media Max with hostile software; such as a trojan version of MMX.exe which installs a back door, or grants Everyone "Full Control" rights to other portions of the system when run.

The attacker then waits for a high rights user, such as an Administrator or a member of Power Users group to spring the trap by logging into the computer and inserting a Media Max CD. When the victim inserts the Media Max CD, the Media Max software automatically launches the attacker subverted "MMX.exe" program with the rights of the current user.

If the attacker is a virus this allows the virus to run as a high rights user. If the attacker is a malicious user, this allows the malicious user to install their back door, or to grant Everyone "Full Control" rights to other portions of the system.

Reproduction:

To avoid exposure to dangerous code, a safe substitute like cmd.exe can be used for testing in place of a back door, virus, or other hostile code. The test system is demonstrated to be vulnerable if a command window (cmd.exe) appears without prompting. Attackers could have substituted any hostile code they pleased.

1. Install a test system running Microsoft Windows 2000 Service Pack 4 or Microsoft Windows XP make sure to patch the machine if you are running on a network.
2. Create a high rights test user account that is in the local Administrators group
3. Create a low rights test user account who is not an administrator.
4. Log in as the high rights test user account
5. Play a Media Max CD (i.e. Sara McLachlan Remix Album Bloom) which should result in Media Max being installed. You should be able to hear the music and see the message "Original CD" in addition to the cover of the Bloom album.
6. Close the application and log out of the computer
7. Log into the computer as the low rights user
8. Replace the MMX.exe program at "c:\Program Files\Common Files\SunnComm Shared\MMX.exe" with the simulated hostile code "cmd.exe" by opening a command shell and typing (all on one line):

```
copy %WINDIR%\system32\cmd.exe "c:\Program Files\Common Files\SunnCom Shared\MMX.exe"
```

9. Log out of the computer
10. Log into the computer as the high rights test user account
11. Insert the Media Max CD that was played in Step 5 (i.e. Sara McLachlan's Bloom album)

12. Note that a command shell (cmd.exe) appears, that is our simulated attacker controlled hostile code. It is running as the interactive user – not the low rights user, which can be verified with Windows Task manager.

Prepared for the Electronic Frontier Foundation on November 29, 2005