



LAUSD ITD Service Desk

Removing The Latest Sleeper Virus/Worm

(Revised: 02/12/09)
© LAUSD ITD Service Desk
333 S. Beaudry Ave. 9th Floor
Phone 213.241.5200

Table of Contents

Latest Sleeper Virus/Worm

Virus Information	3
How To Remove The Sleeper Virus/Worm From Your Computer	3
After Removing The Virus	4
How To Verify Installation	5

Virus Information



W32.Downadup.B is a worm that spreads by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (BID 31874)

Once a system is infected, it will break through system passwords, connect to network drives and continue infecting machines. Access to security websites is blocked.

How To Remove The Sleeper Virus From Your Computer

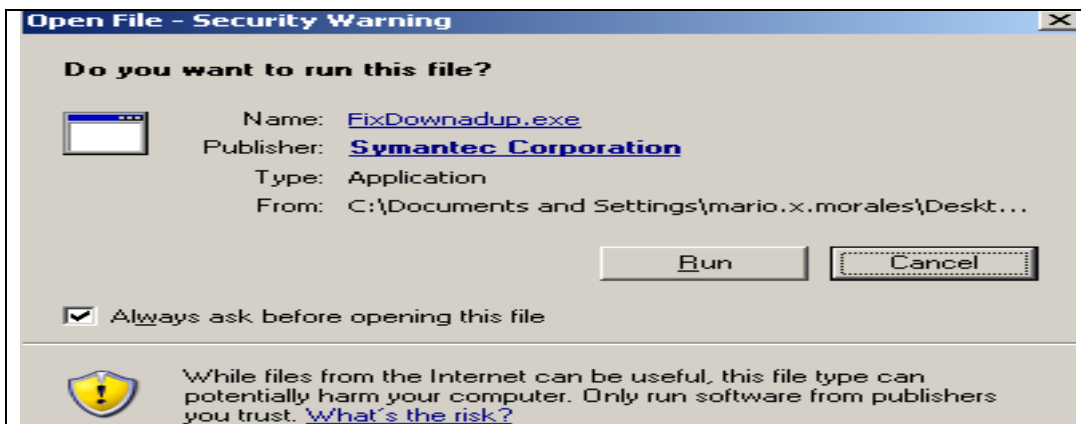
1) Click on the link below and download the tool called "Download Removal Tool" on top of screen and save the executable file to your desktop:

<http://www.symantec.com>

2) After downloading the file. Double click on the icon.



3) Select **RUN**



After Virus Has Been Removed

1) Follow the link below to run the update for “Microsoft Security Bulletin MS08-067”.

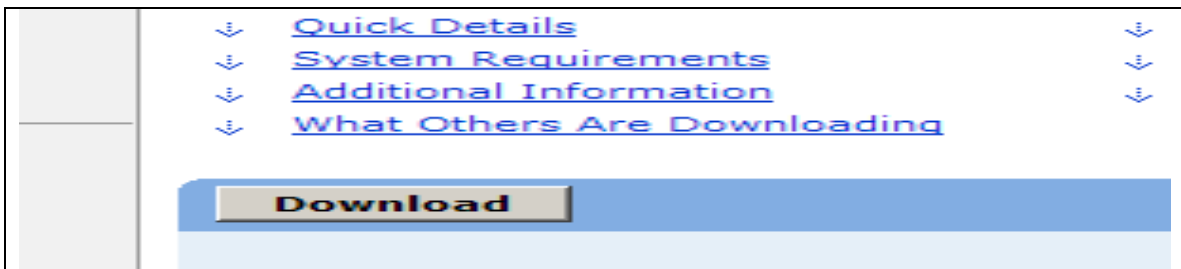
<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>



2) Select the operating system you are currently using.

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Repl by this Update
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 2	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 3	Remote Code Execution	Critical	None

3) Click on **Download**:

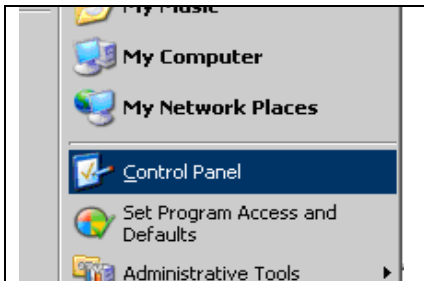


4) After download is complete, double click the executable file and install the update.

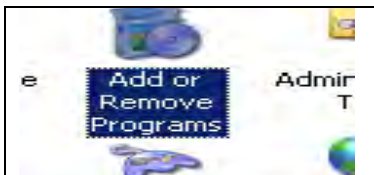


How To Verify The Installation

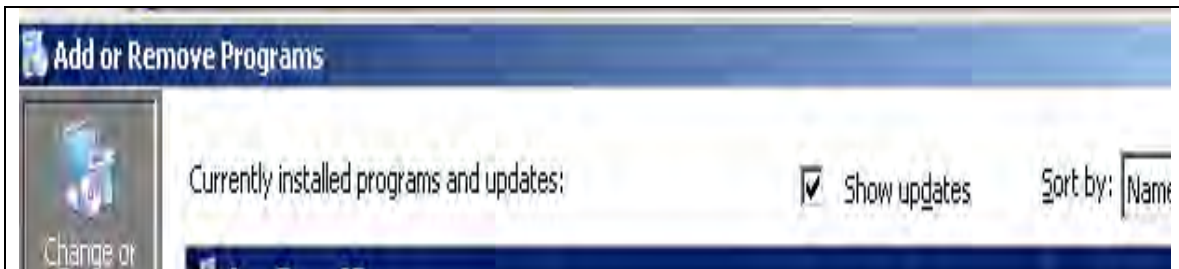
1) Click on **Start**, then **Control Panel**.



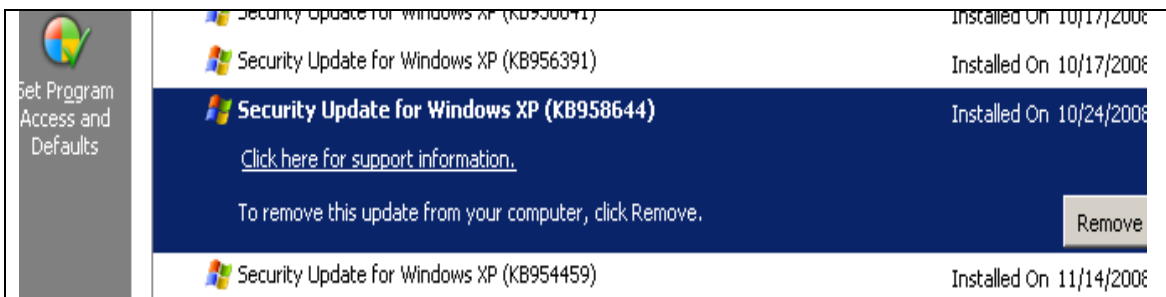
2) Double click on **Add or Remove Programs**.



3) Check the box **Show Updates**.



4) Then look for the "Security Update for Windows XP (KB958644)"



5) You have successfully removed the virus/worm computer once the security update is installed. If you have any questions regarding this document, please call the ITD Service Desk at [213-241-5200](tel:213-241-5200) press menu option 6 then sub-menu option 1 for assistance or visit <http://techsupport.lausd.net> for other support options.