

Windows XP home edition

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-05/2312.html

From: Sadie (*anonymous_at_discussions.microsoft.com*)

Date: 05/14/04

Date: Thu, 13 May 2004 19:33:53 -0700

Was the XP firewall enabled when you tried to update your buddies patches? Or, was your buddy running a third party firewall? Just a tip you might like to pass on for future reference.

Can you access safe mode via the BIOS? I am not 100% certain what is going on here, I am only aware that many people are reporting this type of issue.

This is highly experimental, since I am uncertain what is causing the constant resets being reported by so many people. Virus activity is one possibility—but a multitude of other things such as soundcard problems/CPU overheating can cause resets. Bear in mind, this is written purely from a sense of enabling a P.C to remain online long enough to download critical patches. Let me know if it works or not. My reasoning being, Sasser causes a buffer overrun, flooding lsass. This will be recognised as a system failure, and if set to reboot automatically in the event of system failure, XP will do so.)

If your computer resets before accessing Windows XP, refer to your BIOS manual to determine how to boot into safe mode via the BIOS. (e.g. I tap F5, but your computer may be different.) This may prove impossible—report back, so a clearer picture of events can be garnered from your responses.

To prevent resets interrupting the downloading of patches Turn off Automatic Reboot, if you haven't already. Of course, you can only do this if you can get into Safe Mode and logged in as Administrator:

- 1) Click on "Start", right-click on "My Computer", choose "Properties"
- 2) Click on the "Advanced" tab.
- 3) Under "Startup and Recovery" click on "Settings"

4) Under "System Failure" uncheck "Automatically Restart".

5) Click "Apply" then "Ok" then reboot your system. (If you get an error message, and your system doesn't reboot, report the precise error message.)

If it successfully reboots:

Still in safe mode, run a full virus scan of your entire platform. Decent A.V programmes will allow you to do this.

At the very least, run Stinger, which has been updated to detect all sasser variants. Download and save it straight to a floppy:

Stinger:

<http://vil.nai.com/vil/stinger/>

Bear in mind the possibility that many agobots/worms also exploited the lsass vulnerability. If your buddy got Sasser, he probably let in a few nasties, too. Plus the fact, the lsass patch is not the only patch against remote code execution your pal might've missed.

Beyond that, keep exchanging feedback via this or the virus forum. Even if you elect to reformat, please report whether you were able to accomplish this. By reformat, I mean a true, reboot from CD, run set-up style reformat. It'd really help us all build a clear picture of what is really going on.

Sadie

>-----Original Message-----

>A buddy of mine bought a new Dell Inspiron 5100 with the

>XP OS and didn't hear about the update process being

>important. Guess what he got Sasser. I removed it the

>first time and was in the process of updating his OS

when

>it struck again right in the middle of the installing

the

>security patches. Now the operating system will not come

>up in either regular or safe modes. Am I screwed and

will

>have to reinstall the system and lose all his STUFF as

he

>calls it?

>.

>