

## Sasser question

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-05/1352.html>

---

**From:** Sadie (*anonymous\_at\_discussions.microsoft.com*)

**Date:** 05/16/04

Date: Sun, 16 May 2004 10:43:31 -0700

Hello,Rolando,

It's been a few days since I was reconfonted by this problem.I was desperately trying to resolve the resetting issue,and I am not entirely convinced it is 100% due to Sasser flooding the Isass process.

I spammed these boards for a day or two,trying to probe the exact nature of the problem,but,noone indulged me..Perhaps we can indulge one another?

Here's what I wrote,earlier.The thinking being that the Isass process being overwhelmed would be recognised as a system failure,irrespective of the cause,and prompt an automatic reboot:

"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 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.

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.

FURTHER NOTE: If possible, reboot again into safe mode, run an entire system scan with AV.

Other, possibly applicable articles:

<http://support.microsoft.com/default...kb:en-us:310396>

<http://support.microsoft.com/default...&NoWebContent=1>

I should also have added that after applying the changes whilst in safe mode, you should then attempt to reboot into normal mode, otherwise the modem drivers will not load, and you won't be able to get online..."

That's as far as I got, because nobody responded to indicate whether this would work or not.

Sadie

>-----Original Message-----  
>Please consider indulging a bystander with a friend with a sasser  
>infestation and shutting down so fast that is impossible to do anything else.  
>Are there any files, sasser virus related, that could be deleted or better  
>rename, using the recovery console? (either previously installed or with  
>the installation CD). If a system file is deleted or renamed, the install CD  
>can also be used to be replaced with a simple files repair.  
>This, providing that BIOS is Ok.  
>Cheers  
>  
>  
>---  
>HEARTBURN? WHY? FIX IT!!!  
>HEARTBURN CENTER  
>515-244-9950  
>off\_recreaghmd@hotmail.com  
>To respond, edit out the "off\_" from the address.  
>Para contestar, quite el "off\_" de la direccion.  
>  
>  
>.

>