

XP firewall logs

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-08/0086.html>

From: Tim Chilton – Webtribe (*tim.chilton_at_WEBTRIBE.NET*)

Date: 08/17/04

Date: Tue, 17 Aug 2004 21:09:42 +0100
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Does anyone have any ideas why MS decided to put the firewall log files in the c:\windows directory as a straight text file rather than using the event logs (ie a new firewall log)

Think the logic through

The OS directory is not supposed to be used for temporary files (and I include logs in this). How are we supposed to secure the OS areas if it creates logs there !??

File based logs require NBT ports open so that you can read them remotely, this limits the effectiveness of the firewall.

If event logs were in use, central management via MOM would be possible and all the standard event log handling tools could be used.

Regards

Tim

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.
