

## Re: SQL Server 2000 SP2 xp\_sendmail bug

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-09/0014.html>

---

**From:** Brad Sarsfield (*bradsa\_at\_MICROSOFT.COM*)

**Date:** 09/07/04

Date: Tue, 7 Sep 2004 09:01:36 -0700  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

The problem that Simon is facing can be described as follows:

"xp\_sendmail will fail on a named instance of SQL Server if the instance name is the same name as another service that is running as local system."

This is a bug that we are actively looking at fixing in SQL Server 2000 Service Pack 4.

Thank you for bringing this to Microsoft's attention.

Brad Sarsfield  
Microsoft SQL Server  
bradsa(at)microsoft.com

-----Original Message-----

From: Windows NTBugtraq Mailing List  
[mailto:NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM] On Behalf Of simon edwins (BITS)  
Sent: Thursday, September 02, 2004 3:13 AM  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM  
Subject: SQL Server 2000 SP2 xp\_sendmail bug

We are running Microsoft SQL Server 2000 SP2 (version 8.00.534) on a Windows 2000 Advanced Server with SP3. We have recently discovered a problem which appears to be a bug within SQL when running the xp\_sendmail stored procedure from SQL query analyzer. When we run the xp\_sendmail command with proven correct syntax (the same command works fine on all other SQL servers we have with the same software image) an error message appears stating that the MSSQL services are running under the local system account. I can confirm that both the MSSQL service and SQLAgent services are both set to run using a domain account that has local admin privileges. Additionally, the account the services are set to run under has been configured with a mail profile. The mailbox is hosted on an Exchange 2000 server which allows full access (including send as access) to the account the services are running under. The account has also been granted "Log on as a service" rights. The SQL

NT-Bugtraq: Re: SQL Server 2000 SP2 xp\_sendmail bug

server has been set to use this mail profile, and the test facility reports that it can log on to the profile. I can also confirm that Outlook is indeed the default mail editor on this server, and that using Outlook I can both send and receive emails using the account. The same configuration works fine for all other SQL servers we have.

The investigations I have carried out highlight the cause of the problem. Our SQL installations use instance names which reflect the name of the site to which the SQL server belongs. Our site name is BITS. It appears that when the xp\_sendmail command is run one of the first things that is checked (against the registry) is the server name and the instance name. Once the instance name is known the sqlservr.exe process interrogates the registry for the key HKLM\System\CurrentControlSet\Services\[Instance Name]. [Instance name] is the name of the SQL instance on the server. In our case it is called BITS. On all our other SQL servers this registry key never exists, but here at BITS there is indeed a key called HKLM\System\CurrentControlSet\Services\BITS. This key relates to the BITS (Background Intelligent Transfer Service) service. Once it finds this key it interrogates the property named "ObjectName" and feeds the value found back to the xp\_sendmail procedure. I can confirm this is what happens because when I change the BITS service to run using the same account as SQL the xp\_sendmail procedure runs successfully. In fact, the BITS service doesn't even have to be running, the sqlservr.exe process just reads the information from the registry. The bug appears to be that the sqlservr.exe process searches for a service named [Instance Name] instead of searching for MSSQL\$[Instance Name]. Each SQL server will have a service named MSSQL\$[Instance Name] and the "ObjectName" property will always provide the correct account name. Therefore, this simply seems to be a bug.

I would be grateful to hear if anyone else has discovered this problem or has found a patch to fix it. I have not been able to find any report of this problem within Technet.

Regards

Simon

-----

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.

-----

NT-Bugtraq: Re: SQL Server 2000 SP2 xp\_sendmail bug

-----  
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.

-----