

Re: [VulnDiscuss] Re: Arbitrary Command Execution on Distributor SQL Server 2000 machines (#NISR22002002A)

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

From: Steve (steve@VULNWATCH.ORG)

Date: 08/23/02

Date: Fri, 23 Aug 2002 00:14:45 +0000

From: Steve <steve@VULNWATCH.ORG>

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

<http://www.microsoft.com/technet/security/bulletin/MS02-038.asp> fixes

A buffer overrun vulnerability that occurs in several Database Consistency Checkers (DBCCs) that ship as part of SQL Server 2000. DBCCs are command console utilities that allow maintenance and other operations to be performed on a SQL Server. While many of these are executable only by sysadmin, some are executable by members of the db_owner and db_ddladmin roles as well. In the most serious case, exploiting this vulnerability would enable an attacker to run code in the context of the SQL Server service, thereby giving the attacker complete control over all databases on the server.

A SQL injection vulnerability that occurs in two stored procedures used in database replication. One of these can only be run by users who have been assigned the db_owner role; the other, due to a permissions error, could be run by any user who could log onto the server interactively. Exploiting the vulnerability could enable an attacker to run operating system commands on the server, but is subject to significant mitigating factors as discussed below.

and MS02-043 is (from the MS site)

This is a cumulative patch that includes the functionality of all previously released patches for SQL Server 7.0 and SQL Server 2000. In addition, it eliminates a newly discovered vulnerability.

In the first bulletin MS credits Cesar and in the second they credit David Litchfield and Chip Andrews.

They look pretty similar to me but MS seems to think that these are two separate issues. Has anyone tested the original MS patch MS02-038 to see if it actually fixes the problem?

Regards;

Steve Manzuik
Moderator
VulnDiscuss
VulnWatch

On Thu, 22 Aug 2002, Cesar wrote:

> *This was already published by me one month ago:*
>
> <http://online.securityfocus.com/archive/82/284385>
>
> *and the patch that fix it is:*
>
> <http://www.microsoft.com/technet/security/bulletin/MS02-038.asp>
>
> *All stored procedures vulnerabilities appears in*
> *SecurityHotfix.sql file that is in the above mentioned*
> *patch.*
>
> *Cesar.*
>
> --- David Litchfield <david@ngssoftware.com> wrote:
>> *NGSSoftware Insight Security Research Advisory*
>>
>> *Name: Arbitrary Command Execution on SQL Server 2000*
>> *Systems: Microsoft SQL Server 2000 SP 2*
>> *Severity: High Risk for Distributor servers*
>> *Category: Arbitrary Command Execution*
>> *Vendor URL: <http://www.microsoft.com/>*
>> *Author: David Litchfield (david@ngssoftware.com)*
>> *Advisory URL:*
>>
> http://www.ngssoftware.com/advisories/mssql-sp_MScopyscriptfile.txt
>> *Date: 22nd August 2002*
>> *Advisory number: #NISR22002002A*
>>
>> *Description*
>> *******
>> *A stored procedure on an SQL Server is a series of*
>> *SQL queries that can be*
>> *written once and run many times. One of the internal*
>> *Microsoft stored*
>> *procedures on SQL Server 2000 that the 'public' role*
>> *has permissions to*
>> *execute fails to validate user input before passing*
>> *it to xp_cmdshell. The*
>> *xp_cmdshell extended stored procedure runs an*
>> *operating system command and*
>> *it is possible for a low privileged and malicious*

> > *user to insert and run*
> > *their own arbitrary commands.*
> >
> > *Details*
> > *******
> > *If a Microsoft SQL Server is configured as a*
> > *distributor, so it can*
> > *replicate data between servers, a low privileged and*
> > *malicious user may*
> > *execute the 'sp_MScopyscript' stored procedure and*
> > *insert arbitrary commands*
> > *which will be run in the security context of the SQL*
> > *Server account. If the*
> > *SQL Server is running as LocalSystem then this attack*
> > *will invariably fail.*
> > *The reasons behind this is due to the fact that,*
> > *before the user supplied*
> > *commands are executed, the server must create a*
> > *directory over a network*
> > *share on the distributor. As the Local System*
> > *account has no privileges on*
> > *the network, the stored procedure will fail at this*
> > *point. If the server is*
> > *running in the context of a domain user then the*
> > *"make directory" command*
> > *should work provided replication has been setup*
> > *properly. Once this command*
> > *has executed the stored procedure then inserts the*
> > *user supplied @scriptfile*
> > *parameter into a command: from the text of*
> > *sp_MScopyscript*
> >
> > *select @cmd = N'copy "' + @scriptfile + N"' "' +*
> > *@directory + N"'*
> > *exec @retcode = master..xp_cmdshell @cmd, NO_OUTPUT*
> >
> > *By supplying a malformed @scriptfile parameter an*
> > *attacker can run arbitrary*
> > *commands:*
> >
> > *use master*
> > *declare @cmd nvarchar(4000)*
> > *exec sp_MScopyscriptfile N'c:\autoexec.bat"*
> > *c:\cp.txt&echo hello >*
> > *c:\ccc.bbb & echo 'hello',@cmd OUTPUT*
> > *print @cmd*
> >
> >
> > *The above query will copy the autoexec.bat file to*
> > *cp.txt but also echo*
> > *hello to a file called ccc.bbb.*

NT-Bugtraq: Re: [VulnDiscuss] Re: Arbitrary Command Execution on Distributor SQL Server 2000 machines (#NISR2200

- ***In reply to:*** Cesar: "Re: Arbitrary Command Execution on Distributor SQL Server 2000 machines (#NISR22002002A)"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]

Re: [VulnDiscuss] Re: Arbitrary Command Execution on Distributor SQL Server 2000 machines (#NISR2200