

## Critical Alert Update – W32.Slammer

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2003-01/4906.html>

---

**From:** Jerry Bryant [MSFT] ([jbryant@online.microsoft.com](mailto:jbryant@online.microsoft.com))

**Date:** 01/28/03

From: "Jerry Bryant [MSFT]" <[jbryant@online.microsoft.com](mailto:jbryant@online.microsoft.com)>

Date: Tue, 28 Jan 2003 07:59:34 -0800

Of note in this update, we have begun a list of MSFT products that install MSDE at the following location:

<http://www.microsoft.com/technet/security/MSDEapps.asp>

PSS Security Response Team Alert – Update: W32.Slammer

UPDATED: January 27, 2003

SEVERITY: CRITICAL

DATE: January 25, 2003

PRODUCTS AFFECTED: SQL Server 2000 RTM, SQL Server 2000 SP1, SQL Server 2000 SP2, and Microsoft SQL Desktop Engine Version (MSDE) 2000 RTM, Microsoft SQL Desktop Engine Version (MSDE) SP1, Microsoft SQL Desktop Engine Version (MSDE) 2000 SP2, and all applications that install Microsoft SQL Desktop Engine Version (MSDE) 2000 RTM, SP1 or SP2. A list is provided in the alert below.

\*\*\*\*\*

Update January 27, 2003

This alert has been updated to provide the following additional information:

A list of products that include Microsoft SQL Desktop Engine (MSDE) 2000.

Updated information regarding the availability of downloads for Microsoft SQL Desktop Engine (MSDE) 2000 SP2 and MSDE 2000 SP3. Microsoft has provided these downloads to allow customers to more easily update their MSDE 2000 installations to SP2 or SP3. Customers who are using MSDE 2000, or a product that includes MSDE 2000, must install the SP2 update in order to apply the most recent cumulative SQL Server security patch, Microsoft Security Bulletin MS02-061, which includes the functionality necessary to prevent infection from the W32.Slammer worm.

It is important to note that any customer who has patched their machines with the Microsoft Security Bulletin MS02–039 patch, or any subsequent cumulative SQL security patch, is completely safe from infection from the W32.Slammer. However, Microsoft recommends customers apply Microsoft Security Bulletin MS02–061, which is the most recent cumulative SQL security patch, if they have not applied the patches for Microsoft Security Bulletin MS02–039, MS02–043, or MS02–056. Alternatively, customers may install SQL Server 2000 Service Pack 3 or MSDE 2000 Service Pack 3 which incorporates the patches in Microsoft Security Bulletin MS02–061.

Update January 26, 2003

The Product Support Services Security Team is updating this alert in response to changes in Microsoft Security Bulletin MS02–061.

Microsoft re–released Microsoft Security Bulletin MS02–061 on January 26th, 2003 to include an installer that eliminates the need for system administrators to manually configure the files for the patch. The re–released MS02–061 patch also includes QFE patch Q317748. Both of these changes were made to make it easier for system administrators to configure their system in line with Microsoft's commitment to "secure in deployment" as part of the Trustworthy Computing Initiative. The binaries included in the updated MS02–061 and the Q317748 QFE. Customers who have installed SQL Server 2000 SP3, or MSDE SP3 do not need to install MS02–061.

Customers who have followed previously issued instructions and already installed Microsoft Security Bulletin MS02–039, MS02–043, MS02–056 or MS02–061 do not need to install the new patch in order to prevent the W32.Slammer worm from infecting their machines. Microsoft recommends that customers consider upgrading to Microsoft Security Bulletin MS02–061 in order to patch their machines with the latest SQL Server 2000 cumulative security patch.

Customers who have not yet taken those preventative measures should follow the directions provided in this alert to patch their machines against the vulnerability exploited by the W32.Slammer worm.

#### WHAT IS IT?

The PSS Security Response Team is issuing this alert to inform customers about the W32.Slammer worm, which is currently spreading in the wild. You are not at risk unless you are running one of the above listed products, including any Microsoft products that include and install MSDE 2000. Customers are advised to review this information and take the appropriate action for their environments.

This alert is primarily focused at business customers.

#### IMPACT OF ATTACK:

Denial of Service

#### TECHNICAL DETAILS:

W32.Slammer is a memory resident worm that propagates via UDP Port 1434 and exploits a vulnerability in SQL Server systems and systems with Microsoft SQL Desktop Engine (MSDE) Version 2000 that have not applied the patch released by Microsoft Security Bulletin MS02–039. This bulletin was first available on July 24, 2002.

This worm is designed to propagate, but does not appear to contain any additional payload.

Please contact your Antivirus Vendor for additional details on this worm.

#### PREVENTION:

This worm utilizes a previously–announced vulnerability as part of its infection method. The vulnerability used by the worm to infect machines is discussed at:

<http://www.microsoft.com/technet/security/bulletin/MS02–039.asp>

Microsoft, however, recommends that customers install the most recent cumulative security patch for Microsoft SQL Server 2000 which is Microsoft Security Bulletin MS02–061 (which will also patch MSDE 2000), and which includes the fixes for the vulnerabilities that were announced in Microsoft Security Bulletin MS02–039. MS02–061 can be found at:

<http://www.microsoft.com/technet/security/bulletin/MS02–061.asp>

This patch is also included in Microsoft SQL Server 2000 Service Pack 3.

Due to support issues with certain configurations, customers should install the patch for Microsoft Security Bulletin MS02–061 using the following instructions:

A) If you are running Windows NT 4.0 Server Service Pack 6a install the patch referenced in Microsoft Knowledgebase Q258437, the Microsoft Knowledge Base can be found at <http://support.microsoft.com>.

B) Install the security patch associated with Microsoft Security Bulletin MS02–061. Please note that the Microsoft Security Bulletin MS02–061 was re–released on January 26th, 2003 to include an installer that eliminates the need for system administrators to manually configure the files for the patch. The re–released MS02–061 patch also includes QFE patch Q317748. Both of these changes were made to make it easier for system administrators to configure their system in line with Microsoft's commitment to "secure in deployment" as part of the Trustworthy Computing Initiative. The binaries included in the updated MS02–061 and the Q317748 QFE. Customers who have installed SQL Server 2000 SP3 do not need to install MS02–061.

C) Users can verify installation of this patch by verifying the following files are at version 8.00.568:  
ssmslpcn.dll

dbmslpcn.dll

If you cannot apply this patch immediately, the following options can limit propagation of the worm:

- A) Block UDP port 1434 inbound and outbound traffic at your firewalls.
- B) You may also block UDP port 1434 inbound traffic on your Microsoft SQL 2000 Servers or Microsoft SQL Desktop Engine (MSDE) Version 2000. Following this instruction may result in support issues as this port performs name resolution.

Installation of these patches will prevent infection by the W32.Slammer Worm.

Microsoft SQL Desktop Engine (MSDE) 2000 Detection:

The link below contains a list of products that include Microsoft SQL Desktop Engine (MSDE) 2000

<http://www.microsoft.com/technet/security/MSDEapps.asp>

It is important that customers who use products that include MSDE 2000 check to see if they have MSDE installed, and in the case that they do, verify that their installation has been updated in one of the following ways:

Installation of MSDE 2000 SP2 and patch associated with Microsoft Security Bulletin MS02-039, MS02-043, MS02-056, or MS02-061.

Installation of MSDE 2000 SP3.

Customers using any of these products can also detect if they have Microsoft SQL Desktop Engine (MSDE) 2000 installed by using the following instructions:

Go to "Start" then "Search" and search the local system for the file "sqlservr.exe". If this file is present on your system, then you have MSDE or SQL Server installed. Next right click on this file and select "properties" then "product version". If the product version is between 8.00.0194 and 8.00.0533 you are running SQL Server 2000 or MSDE 2000 you need to install SQL Server 2000 SP2 before you install this patch.

If the product version is between 8.00.0534 and 8.00.0636 then you are running SQL Server 2000 or MSDE 2000 and need either the updates provided in Microsoft Security Bulletin MS02-061 or SQL Server 2000 SP3 or MSDE 2000 SP3. SQL Server 2000 SP3 and MSDE 2000 SP3 include the fixes in Microsoft Security Bulletin MS02-061.

Microsoft SQL Desktop Edition (MSDE) 2000 Additional Information:

Customers who have Microsoft SQL Desktop Edition must update their Microsoft SQL Desktop Edition (MSDE) 2000 to Service Pack 2 to install the security

## microsoft.public.sqlserver.security: Critical Alert Update – W32.Slammer

patch associated with Microsoft Security Bulletin MS02–061. Customers can also install Microsoft SQL Desktop Edition Service Pack 3, but as always Microsoft recommends they thoroughly test it before deployment. Download locations for Microsoft SQL Desktop Edition (MSDE) 2000 SP2 and SP3 are available now in Microsoft Security Bulletin MS02–061.

### RECOVERY:

Instructions for Removal of W32.Slammer from infected Microsoft SQL Server 2000 Servers or Microsoft SQL Desktop Edition (MSDE 2000)

Set the SQL Server Service to Manual.

Reboot the infected machine.

If you are running Windows NT 4.0 Server Service Pack 6a install the patch referenced in Microsoft Knowledgebase Q258437. The Microsoft Knowledge Base can be found at <http://support.microsoft.com>.

Install the security patch associated with Microsoft Security Bulletin MS02–061. Please note that the Microsoft Security Bulletin MS02–061 was re–released on January 26th, 2003 to include an installer that eliminates the need for system administrators to manually configure the files for the patch. The re–released MS02–061 patch also includes QFE patch Q317748. Both of these changes were made to make it easier for system administrators to configure their system in line with Microsoft's commitment to "secure in deployment" as part of the Trustworthy Computing Initiative. The binaries included in the updated MS02–061 and the Q317748 QFE. Customers who have installed SQL Server 2000 SP3 do not need to install MS02–061.

Users can verify installation of this patch by verifying the following files are at version 8.00.568:

ssmslpcn.dll  
dbmslpcn.dll

Set the SQL Server Service to Automatic.

If you need further assistance regarding this worm, please contact Microsoft Product Support Services, or your preferred antivirus vendor.

### RELATED KB ARTICLES:

<http://support.microsoft.com?kbid=813440>

An updated article will be made available within 24 hours.

### RELATED MICROSOFT SECURITY BULLETINS:

Customers should install the re–released cumulative security patch for Microsoft SQL Server 2000, which includes the fixes for the vulnerabilities that were announced in Microsoft Security Bulletin MS02–039. The patch can be found here:

<http://www.microsoft.com/technet/security/bulletin/MS02-061.asp>

Customers who have previously installed the patches for Microsoft Security Bulletin MS02-039, MS02-043, MS02-056, MS02-061 do not need to install this new patch.

Customers may install Microsoft SQL Server SP3 or Microsoft SQL Desktop Edition (MSDE) 2000 SP3 which includes the patch associated with Microsoft Security Bulletin MS02-061. As always, customers should thoroughly test SP3 before installation. Before installing either SQL Server 2000 SP3 or Microsoft SQL Desktop Edition (MSDE) 2000 SP3 you should set the SQL Server Service to Manual and reboot the machine to ensure the installation succeeds.

Customers with Application Center 2000 should follow the instructions in the following KnowledgeBase Article to allow for installation of the updated patch for Microsoft Security Bulletin MS02-061:  
<http://support.microsoft.com?kbid=813115>

#### ADDITIONAL INFORMATION

As always, please make sure to enable a firewall and use the latest Anti-Virus detection from your Anti-Virus vendor to prevent and detect new viruses and their variants.

If you have any questions regarding this alert please contact your Microsoft representative or 1-866-727-2338 (1-866-PCSafety) within the US, outside of the US please contact your local Microsoft Subsidiary.

PSS Security Response Team

--

Regards,

Jerry Bryant - MCSE, MCDBA

Microsoft IT Communities

Get Secure! [www.microsoft.com/security](http://www.microsoft.com/security)

This posting is provided "AS IS" with no warranties, and confers no rights.