

## MICROSOFT SQL SERVER VULNERABILITIES

---

The following Microsoft SQL Server vulnerabilities and their recommended remedies are discussed in this technical bulletin:

- SQL Slammer
- What Should Security Analyzer Customers Do?
- What Should VigilEnt Customers Do?
- Finding SQL Slammer with VSA for SQL Server
- Related Links

## Microsoft SQL Server Vulnerabilities

---

### SQL SLAMMER

The recent SQL W32.Slammer worm, also known as SQL Slammer or Slammer, infects SQL Server port 1434, the default Microsoft SQL Server UDP port.

The affected products are:

- ◆ Microsoft SQL Server 2000
- ◆ Microsoft Desktop Engine (MSDE) 2000

In July 2002, Microsoft issued Microsoft Security Bulletin MS02-039 to address a buffer overflow issue with SQL Server's Resolution Service, which listens on UDP port 1434. The Resolution Service was introduced in SQL Server 2000 to support multiple instances of SQL Server running on the same machine. The SQL Slammer worm exploits a Resolution Service vulnerability by feasting on SQL Server instances that do not have the latest Service Pack (SP 3) or comparable patches installed.

**Note from Microsoft:** Microsoft SQL Server customers who have patched their machines with the Microsoft Security Bulletin MS02-039 patch, or any subsequent cumulative SQL security patch, are completely safe from infection from the W32.Slammer worm. However, Microsoft recommends customers apply Microsoft Security Bulletin MS02-061, which is the most recent cumulative SQL Server 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.

### WHAT SHOULD SECURITY ANALYZER CUSTOMERS DO?

Security Analyzer (SA) already checks for the two patches that Microsoft provides to protect against the Slammer worm. In addition, a new security test has been added that checks to determine w32.Slammer vulnerabilities.

SA customers should run an AutoSync first, then run the Database Services Analysis scan profile against their database target host. A new security test called SQL Slammer Worm Vulnerability has been added to the Database Services Analysis profile that checks to see if a system has not applied the related patches (MS02-039 and MS02-034). If these patches have not been installed, the customer is alerted to their vulnerability to the SQL Slammer worm.

### WHAT SHOULD VIGILENT CUSTOMERS DO?

The following VigilEnt Enterprise Security Applications require or optionally use MSDE or SQL Server as their database management system:

- ◆ VigilEnt Policy Center
- ◆ VigilEnt Security Manager
- ◆ VigilEnt Log Analyzer
- ◆ VigilEnt User Manager
- ◆ VigilEnt Password Manager

VigilEnt customers should ensure that they have the latest Microsoft SQL Server service packs and security patches downloaded and installed at all times.

If you installed the version of MSDE that came with the VigilEnt product, you are safe from the Slammer worm, as that version of MSDE is not one of the versions affected by the worm.

### PROBLEMS?

Call NetIQ Technical Support at  
**888.283.4840** or **713.860.9777**

**Product Patch**  
**January 28, 2003**

Copyright © 2003 NetIQ Corporation. All rights reserved.

Product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

If you are running SQL Server 2000 as a backend for your VigilEnt products, you must install at least Service Pack 2. If you install Service Pack 2, you must also download and install the SQL Server 2000 Security Update for Service Pack 2 from <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316333&sd=tech>. If you choose, you can install Service Pack 3 instead, which includes the security fixes and does not require a security update download.

If you are running SQL Server 7, you should install Service Pack 4. Then download and install the cumulative security patch located at: <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q327068&sd=tech>.

VSM customers should use VSM in conjunction with VSA for SQL Server to identify SQL Server instances that are potentially vulnerable to the Slammer worm.

## FINDING SQL SLAMMER WITH VSA FOR SQL SERVER

NetIQ has released a product patch for VigilEnt Security Agent for SQL Server to help customers easily identify SQL Server instances that are vulnerable to the W32.Slammer worm. VSA for SQL Server customers may download this patch from the NetIQ SupportWeb and run a security checkup report through VSM to check the patch levels across all enterprise SQL Server instances.

To check the patch levels, run a security checkup report that contains the **Latest SQL Server Patch Installed** security check. If the value for the security check is **true**, then you have the latest SQL Server patch installed, and your SQL Server instances are safe from the Slammer worm.

## RELATED LINKS

- ◆ <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/alerts/slammer.asp>
- ◆ <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-061.asp>
- ◆ <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp>
- ◆ CAN/CVE Buffer Overflow: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0649>
- ◆ CAN/CVE Denial of Service: <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0650>