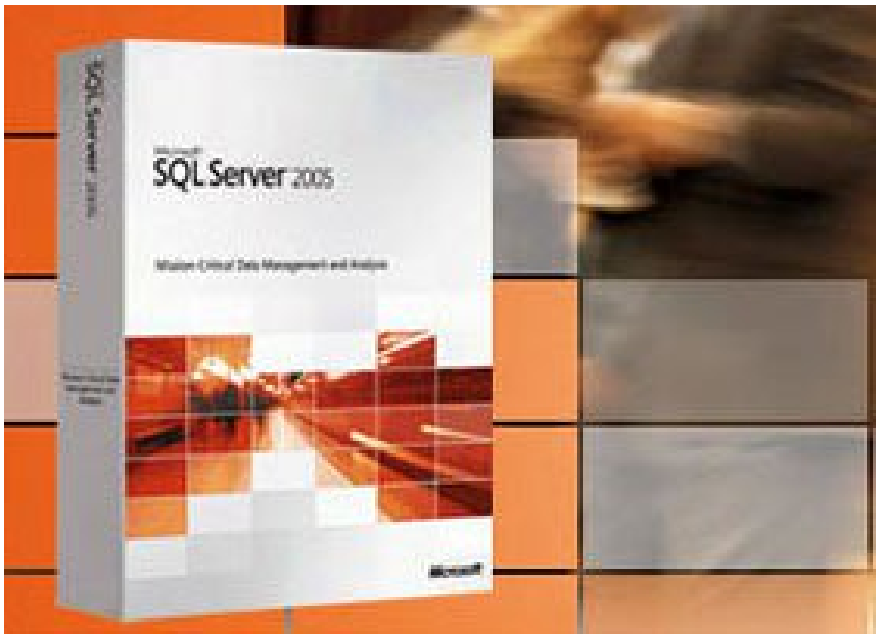
Warning about serious vulnerabilities in SQL Server

Systems running SQL Server 2000, SQL Server 2005, SQL Server 2005 Express Edition, SQL Server 2000 Desktop Engine (MSDE 2000), ... can be exploited and controlled

Microsoft has announced yesterday that an attack code has been issued aimed at a serious vulnerability in previous versions of its SQL Server database software, besides Microsoft. It also advises users to use this temporary solution.



This security error was first reported to Microsoft in April 2008 by an Austrian security consulting company called SEC Consult. However, the company says it can't wait for Microsoft to decide when to release the patch and has revealed the flaw in the past two weeks with the release of proof-of-concept exploit code.
According to SEC Consult, Microsoft may already have a patch ready in the last three months but has not released a patch yet.

On Microsoft, in a security advisory released on Monday, Microsoft also said that systems running SQL Server 2000, SQL Server 2005, SQL Server 2005 Express Edition, and SQL Server 2000 Desktop Engine (MSDE 2000), Microsoft SQL Server 2000 Desktop Engine (WMSDE) and Windows Internal Database (WYukon) can be exploited and controlled by hackers.

This error has been detected in the SQL Server "sp_replwritetovarbin" extension stored procedure.

However, recent versions of this popular software, used for many Web sites to provide more power to their back-end databases, are not attacked. These versions include SQL Server 7.0 Service Pack 4 (SP4), SQL Server 2005 SP3 and SQL Server 2008. The latest, most recent version of this product line has been released to manufacturers from the end. August.

As the previous moves, Microsoft has taken actions to reduce their losses. 'We already know the exploit code is published on the Internet. Still, it has not been seen about any attacks trying to use the reported vulnerability, 'said company spokesman Bill Sisk in an email Monday.

Attackers can exploit this vulnerability remotely if they are able to increase access to the server through SQL injection attacks on the Web application on the system, Sisk said.

SQL injection attacks were successful; Hackers have taken control to compromise a large number of sites, even famous commercial domain names, with such attacks. Thousands of legitimate sites have been hacked through SQL injection attacks in recent weeks by criminal organizations, after which hackers have plugged fake code into their pages and attacked visitors. Use Internet Explorer (IE). In this security flaw, Microsoft blocked the flaw in IE last Wednesday with a second emergency patch within two months.

Microsoft has said that refusing the terms for the "sp_replwritetovarbin" extension stored procedures will create a vulnerability for the system, and also provide instructions on how to implement against attacks. this.

However, Sisk did not commit a fix or a timeline to the fix, but he proved - 'Microsoft will continue to study the flaw and proceed to finalize this research, in the process. Research, the company will take appropriate actions' - typical instructions at some point for the patch.

However, SEC Consult has made claims to Microsoft to complete the revision in September.

The Vienna-based company published the vulnerability in 9.12 through a published information, along with a sample attack code in an advisory section on their site, as well as several secure mailing lists: Bugtraq and Full Disclosure.

Also in this disclosure, SEC Consult said that it was announced by Microsoft in September via a mail that the patch has been completed. However, 'The release schedule for this fix has not been announced'.

This Austrian security company also included a timeline reflecting communication between the company and Microsoft. At that time table, SEC Consult reported this vulnerability to Microsoft on April 17, 2008 and the most recent response from Microsoft was on September 29. Four times since then 14.10, 29.10, 12.11 and 28.11 - SEC Consult questioned Microsoft about the patch upgrade but never received feedback from Microsoft.

Microsoft did not respond to SEC Consult's questions about the availability of its patch and timeline.

You finished reading the article "**Warning about serious vulnerabilities in SQL Server**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com