

[VulnWatch] Microsoft SQL Server 2000 'BULK INSERT' Buffer Overflow (#NISR11072002)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-07/0021.html>

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

Date: 07/11/02

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

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

Date: Thu, 11 Jul 2002 15:28:52 +0100

NGSSoftware Insight Security Research Advisory

Name: BULK INSERT Buffer Overflow

Systems Affected: Microsoft SQL Server 2000

Severity: Medium

Category: Buffer Overrun

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

Authors: Mark Litchfield (mark@ngssoftware.com)

Advisory URL: <http://www.ngssoftware.com/advisories/ms-sqlbi.txt>

Date: 11th July 2002

Advisory number: #NISR11072002

VNA Reference: <http://www.nextgenss.com/vna/ms-sql.txt>

[Please note that this advisory relates to one of the issues discussed in the SQL Server VNA. There are still more to be fixed.]

Description

Microsoft's SQL Server 2000 contains functionality that allows a database owner to populate a table with data with one fell swoop using the 'BULK INSERT' query. This functionality contains a remotely exploitable buffer overrun vulnerability that can be exploited by an attacker to run arbitrary code.

Details

The 'BULK INSERT' query will take a user supplied file name and insert the contents of this file into a specified table. By supplying an overly long filename to the query, a buffer is overflowed and the saved return address stored on the stack is overwritten. This allows the attacker to gain control over the process' execution. SQL Server 2000 can be run in the security context of a domain account or LOCAL SYSTEM, so depending upon the particular setup, an attacker may be able to gain complete control over the vulnerable system.

VulnWatch: [VulnWatch] Microsoft SQL Server 2000 'BULK INSERT' Buffer Overflow (#NISR11072002)

To be able to use the 'BULK INSERT' query one must have the privileges of the database owner or dbo. Note this does not necessarily imply 'sa' equivalence.

Another point to note is that whilst this overflow is 'UNICODE' in nature by supplying code as a UNICODE string exploitation is made easier.

Fix Information

NGSSoftware alerted Microsoft to this problem on the 28th May 2002. Microsoft have created a patch.

Please see their bulletin for more details:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-034.asp>

Whilst NGSSoftware rate this as a medium risk issue, we still urge customers to apply the patch as soon as is possible as it contains fixes for other issues such as a buffer overflow in the `pwdencrypt()` function.

Further Information

For further information about the scope and effects of buffer overflows, please see

<http://www.ngssoftware.com/papers/non-stack-bo-windows.pdf>
<http://www.ngssoftware.com/papers/ntbufferoverflow.html>
<http://www.ngssoftware.com/papers/bufferoverflowpaper.rtf>
<http://www.ngssoftware.com/papers/unicodebo.pdf>

- **Previous message:** [Marc Maiffret: "\[VulnWatch\] EEYE: Remote PGP Outlook Encryption Plug-in Vulnerability"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)