

# [NT] BULK INSERT Buffer Overflow

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0044.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 07/11/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Thu, 11 Jul 2002 22:03:41 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

BULK INSERT Buffer Overflow

---

## SUMMARY

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.

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.

## Securiteam: [NT] BULK INSERT Buffer Overflow

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 28 May 2002. Microsoft has 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>>  
<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.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@nextgenss.com>>  
NGSSoftware Insight Security Research.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] XSS Hole in Fluid Dynamics Search Engine"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)