

# [NT] Unchecked Buffer in Network Share Provider Can Lead to Denial of Service

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0089.html>

---

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

*Date:* 08/23/02

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

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

Date: Fri, 23 Aug 2002 22:58:21 +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.

-----

Unchecked Buffer in Network Share Provider Can Lead to Denial of Service

---

## SUMMARY

SMB (Server Message Block) is the protocol Microsoft uses to share files, printers, serial ports, and to communicate between computers using named pipes and mail slots. In a networked environment, servers make file systems and resources available to clients. Clients make SMB requests for resources and servers make SMB responses in what described as a client server, request-response protocol.

By sending a specially crafted packet request, an attacker can mount a denial of service attack on the target server machine and crash the system. The attacker could use both a user account and anonymous access to accomplish this. Though not confirmed, it may be possible to execute arbitrary code.

## DETAILS

Affected Software:

- \* Microsoft Windows NT 4.0 Workstation
- \* Microsoft Windows NT 4.0 Server
- \* Microsoft Windows NT 4.0 Server, Terminal Server Edition
- \* Microsoft Windows 2000 Professional

## Securiteam: [NT] Unchecked Buffer in Network Share Provider Can Lead to Denial of Service

- \* Microsoft Windows 2000 Server
- \* Microsoft Windows 2000 Advanced Server
- \* Windows XP Professional

### Mitigating factors:

- \* An administrator can block this attack by turning off anonymous access. However, this does not prevent legitimate users from exploiting this vulnerability.
- \* An administrator can block access to SMB ports from untrusted networks. By blocking TCP ports 445 and 139 at the network perimeter, administrators can prevent this attack from untrusted parties. In a file and printing environment, this may not be a practical solution for legitimate users.
- \* An administrator can stop the Lanman server service which prevents the attack, but again may not be suitable on a file and print sharing server.

### Patch availability:

#### Download locations for this patch

- \* Microsoft Windows NT 4.0:

<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41493>  
<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41493>

- \* Microsoft Windows NT 4.0 Terminal Server Edition:

<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41519>  
<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41519>

- \* Microsoft Windows 2000:

<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41468>  
<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41468>

- \* Microsoft Windows XP:

<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41524>  
<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41524>

- \* Microsoft Windows XP 64 bit Edition:

<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41549>  
<http://www.microsoft.com/downloads/Release.asp?ReleaseID=41549>

### What's the scope of the vulnerability?

This is a denial of service attack. By sending a specially crafted packet request to a computer, an attacker can crash the system of the target machine. The attacker could use both a user account and anonymous access to accomplish this. Though not confirmed, it may be possible to execute arbitrary code.

If system administrators have turned off anonymous access, it would not be possible for a non-authenticated user to exploit this vulnerability. However, turning off anonymous access does not prevent authenticated users from this attack.

In addition, an administrator can block access to SMB on TCP ports 445 and 139 at the network perimeter. This would block access from untrusted

## Securiteam: [NT] Unchecked Buffer in Network Share Provider Can Lead to Denial of Service

networks. However, legitimate users could be blocked in a file and print networking environment.

Administrators could also shut down the Lanman server service. However, in a file and print networking environment this may not be a viable solution because it would block legitimate users from using file and print services on a particular server where the Lanman service had been stopped.

What causes the vulnerability?

The vulnerability results because of a flaw in the way Microsoft's implementation of SMB receives a packet requesting the SMB service.

What is SMB?

SMB (Server Message Block) is the protocol Microsoft uses to share files, printers, serial ports, and to communicate between computers using named pipes and mail slots. In a networked environment, servers make file systems and resources available to clients. Clients make SMB requests for resources and servers make SMB responses in what described as a client server, request–response protocol.

What's wrong with the SMB implementation?

There is an unchecked buffer in a section of code that requests the SMB service.

What could this vulnerability enable an attacker to do?

This vulnerability could enable an attacker launch a denial of service attack against vulnerable systems either locally or remotely using either a user account or anonymous access.

But this is a buffer overrun vulnerability. Don't they usually allow the attacker to run code on the system?

Normally this is true. However, in the testing process, neither the development team nor the reporter was able to find a way for an attacker to run code on the system. This does not mean that it is not possible, just that testing so far has not yielded this result. Again, administrators are encouraged to apply the patch.

How could an attacker exploit this vulnerability?

An attacker could seek to exploit this vulnerability on machines that have anonymous access enabled by sending a malformed SMB request to a target computer and crashing it.

Could this vulnerability be exploited by a user on the Internet?

Only if TCP ports 445 and 139 were open at the firewall. This would block access from untrusted networks. Best practices say these ports should be blocked.

Would the user need to be authenticated in order to exploit the vulnerability?

If anonymous access has been disabled, only an authenticated user could exploit this vulnerability. Requiring authenticated users instead of

Securiteam: [NT] Unchecked Buffer in Network Share Provider Can Lead to Denial of Service

anonymous access would make it easier for an administrator to determine who the attacker was.

What does the patch do?

The patch eliminates the vulnerability by checking for correct inputs before responding to SMB requests, thereby eliminating the vulnerability.

ADDITIONAL INFORMATION

The information has been provided by

<[mailto:0\\_35556\\_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C\\_US@Newsletters.Microsoft.com](mailto:0_35556_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com)>  
Microsoft Product Security.

=====

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): "[TOOL] ComLog.pl, a WIN32 Command Prompt Logger"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)