

# [NT] Microsoft Windows 2000 SNMP Memory Utilization DoS

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0106.html>

---

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

*Date:* 10/22/02

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

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

Date: 22 Oct 2002 20:24:54 +0200

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.

-----

Microsoft Windows 2000 SNMP Memory Utilization DoS

---

## SUMMARY

If the SNMP service is running on a Windows 2000 server, and the 'Print Spooler' service is not running, repeatedly using SNMP queries to obtain print queue related values in the LANMAN MIB will cause the SNMP service to consume very large amounts of memory. It is necessary to have a valid 'read' string in order to carry out the attack. The default read string is 'public'.

Approximately 30MB of memory is allocated per SNMP request received.

## DETAILS

Vulnerable systems:

- \* Windows 2000 Server SP2 (Immib2.dll, file version 5.00.2134.1)

Immune systems:

- \* Windows 2000 Server SP3

Impact:

An attacker can cause the SNMP service to consume all available memory on the server, causing the server to stop responding until rebooted. Under certain circumstances it may be necessary to power down the server rather

## Securiteam: [NT] Microsoft Windows 2000 SNMP Memory Utilization DoS

than executing a 'graceful' shutdown.

### Technical Details:

The LAN Manager (LANMAN) MIB is installed automatically with the Windows 2000 SNMP Agent. The LANMAN MIB is implemented by Immib2.dll.

If the SNMP Agent service (SNMP.exe) is running and the "print spooler" service (spoolsv.exe) has not been started since the SNMP Service was started, a 'GET' or 'GETNEXT' request to the SNMP Agent will cause the LANMAN SNMP Extension to leak a very large amount of memory (in tests approximately 30MB per request).

A valid 'read' string is necessary to perform the attack; in a typical network attack this could be obtained by sniffing a network, by examining the configuration of a compromised host such as a workstation, or by guesswork; typically SNMP community strings are not changed frequently.

The attack can be performed using an SNMP manager utility such as the SNMPUtil tool provided in the Windows 2000 resource kit. Example command lines follow:

(using the NGS Software SNMP utility, 'snmplib')

```
snmplib get <hostname> 161 public 1.3.6.1.4.1.77.1.2.28.0
```

(using the SNMPUtil tool)

```
snmputil getnext localhost public .1.3.6.1.4.1.77.1.2.28.0
```

The effect of the attack can be observed using the Windows 2000 task manager application; add the 'VM Size' column to the 'Processes' window using the 'View/select columns' menu option.

When the attack is repeated several times performance of the server will begin to severely degrade, resulting in the inability to start new processes or allocate memory. Different programs will fail in different ways, however an especially unfortunate failure mode is encountered if a user attempts to log on and mistypes the password; a failure to allocate memory in the WinLogon process causes the logon GUI to freeze.

More Information on this vulnerability is available at:

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q296815>>  
<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q296815>

### Fix Information:

- Apply the vendor patch (This bug is fixed in Windows 2000 SP3).
- Ensure that only specified management stations are permitted to issue SNMP requests. This can be achieved in Windows 2000 using the 'services' management console plug-in. The SNMP service has a number of configuration pages, one of which is 'security'. This page can be used to specify the hosts (by IP address) from which to accept SNMP packets. This is only a

Securiteam: [NT] Microsoft Windows 2000 SNMP Memory Utilization DoS

mitigation however, since SNMP is a UDP based protocol and the source address of a request can be easily spoofed.

-If possible, implement an IPSec tunnel between management stations and managed Windows 2000 servers.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[chris@ngssoftware.com](mailto:chris@ngssoftware.com)> Chris Anley of Next Generation Security Software.

=====

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): "[NT] Vulnerable Cached Objects in IE (9 advisories in 1)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)