

[NT] Unchecked Buffer in SNMP Service Could Enable Arbitrary Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0078.html>

From: support@securiteam.com

Date: 02/13/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 13 Feb 2002 13:41:48 +0100 (CET)

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 SNMP Service Could Enable Arbitrary Code Execution

SUMMARY

Simple Network Management Protocol (SNMP) is an Internet standard protocol for managing disparate network devices such as firewalls, computers, and routers. All versions of Windows, except for Windows ME, provide an SNMP implementation, which is neither installed nor running by default in any version.

A buffer overrun is present in all implementations. By sending an especially malformed management request to a system running an affected version of the SNMP service, an attacker could cause a denial of service. In addition, it is possible that he cause code to run on the system in LocalSystem context. This could potentially give the attacker the ability to take any desired action on the system.

A patch is under development to eliminate the vulnerability. In the meantime, Microsoft recommends that customers who use the SNMP service disable it temporarily. Patches will be available shortly, at which time we will re-release this bulletin with updated details.

DETAILS

Securiteam: [NT] Unchecked Buffer in SNMP Service Could Enable Arbitrary Code Execution

Affected software:

- * Microsoft Windows 95
- * Microsoft Windows 98
- * Microsoft Windows 98SE
- * Microsoft Windows NT 4.0
- * Microsoft Windows NT 4.0 Server, Terminal Server Edition
- * Microsoft Windows 2000
- * Microsoft Windows XP

Mitigating factors:

- * The SNMP service is neither installed nor running by default in any version of Windows.
- * Standard firewalling practices recommend blocking the port over which SNMP operates (UDP ports 161 and 162). If these recommendations have been followed, the vulnerability could only be exploited by an intranet user.
- * Standard security recommendations recommend against using SNMP except on trusted networks, as the protocol, by design, provides minimal security.

Patch availability:

Download locations for this patch

- * A patch is under development and will be available shortly. When this happens, we will re-release this bulletin with information on how to obtain and install the patch.

What's the scope of the vulnerability?

This is a buffer–overflow vulnerability. If a particular service had been installed and was running on an affected system, it could be possible for an attacker to cause a denial of service on the system. In addition, it is possible that they could run code of their choice.

The service at issue in this vulnerability is neither installed nor running by default on any version of Windows. In addition, the circumstances under which the vulnerability could be exploited would likely prevent it from being exploited by an Internet–based attacker.

What causes the vulnerability?

The vulnerability results because the component of the SNMP agent service that parses incoming commands contains an unchecked buffer. By sending an especially malformed request, it could be possible to conduct a buffer overflow attack against an affected system.

What is SNMP?

SNMP (Simple Network Management Protocol) allows administrators to remotely manage network devices such as servers, workstations, routers, bridges, firewalls, and so forth. SNMP is an industry–standard protocol, which allows devices made by many different vendors to be managed via the protocol.

How does SNMP work?

In order for an administrator to use SNMP, there has to be an agent – that

Securiteam: [NT] Unchecked Buffer in SNMP Service Could Enable Arbitrary Code Execution

is, a service that listens for commands and executes them – on every machine that needs to be managed. Next, the administrator needs to know a password (known in SNMP parlance as a community name) that provides either read-only or read-write access, as appropriate. When the administrator issues a management command, the SNMP software on his system refers to a database (called the Management Information Base) that translates those commands to one that will be meaningful to the other machine.

How secure is SNMP?

SNMP is, by design, not a secure protocol. For instance, all communications in SNMP take place in plaintext, so community names and other potentially sensitive information could potentially be determined by monitoring the network. Microsoft has long recommended using other, more secure methods of managing networks, and this is why the SNMP agent service that ships with Windows platforms is neither installed nor running by default.

What Windows products provide SNMP support?

An SNMP agent service is included in Windows 95, Windows 98, Windows 98SE, Windows NT 4.0, Windows 2000, and Windows XP. However, it is neither installed nor running by default in any of them. Windows ME does not provide an SNMP service of any kind.

Which products' SNMP services are affected by the vulnerability?

All SNMP services are affected. This includes Windows 95, Windows 98, Windows 98SE, Windows NT 4.0 and Windows 2000, and Windows XP.

What's wrong with the SNMP implementations in the affected products?

The SNMP implementations in the affected products have an unchecked buffer in a part of the software that processes management requests. If the SNMP agent service received a management request that is malformed in a particular way, the effect would be to overrun the buffer. If the data in the management request were carefully chosen, it would have the effect of altering the operation of the SNMP service while it was running.

What would this enable an attacker to do?

An attacker who successfully exploited this vulnerability could cause a denial of service in the SNMP service. In addition, it is possible that they could change the operation of the SNMP service. Because it runs as part of the operating system, this would potentially give the attacker complete control over the system.

Who could exploit the vulnerability?

To exploit the vulnerability, the attacker would need to be able to deliver SNMP management requests to the SNMP Service.

How difficult would it be for the attacker to deliver SNMP Management requests to an affected system?

It is likely that an attacker located within a network could deliver SNMP management requests to most other systems on the network, since SNMP operates over TCP/IP. However, if normal firewalling has been performed,

Securiteam: [NT] Unchecked Buffer in SNMP Service Could Enable Arbitrary Code Execution

it might be impossible for an attacker located on the Internet to deliver management requests to a system behind the firewall, as standard firewalling recommendations include blocking UDP ports 161 and 162, the ports over which SNMP traffic travels.

How likely is it that a web server or other Internet–exposed system would be vulnerable?

If best practices have been followed, SNMP would not be used on an Internet–exposed machine. As we discussed above, SNMP is not a secure protocol, and as a result, it is never appropriate to use SNMP to manage a system on the Internet.

Why isn't there a patch for the vulnerability?

A patch is under development to eliminate the vulnerability, but the issue was made public before it could be completed. As a result, we recommend that customers affected by the vulnerability temporarily disable the SNMP service.

How do I disable the SNMP service?

Just follow the steps for the system you are using.

Windows 95, 98 and 98SE:

- * In Control Panel, double–click Network.
- * On the Configuration tab, select Microsoft SNMP Agent from the list of installed components.
- * Click Remove

Check the following keys and confirm that snmp.exe is not listed.

- *
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- * HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Windows NT 4.0 (including Terminal Server Edition):

- * Select Start, then Settings.
- * Select Control Panel, then click on the Services Icon
- * Locate SNMP on the list of services, then select it and click Stop.
- * Select Startup, and click Disabled.
- * Click OK to close the dialogue, then close Control Panel

Windows 2000:

- * Right–click on My Computer and select Manage
- * Click on Services and Applications, then on Services
- * Location SNMP on the list of services, then select it and click Stop.
- * Select Startup, and click Disabled.
- * Click OK to close the dialogue, and then close the Computer Management window.

Windows XP:

- * Right–click on My Computer and select Manage
- * Click on Services and Applications, then on Services
- * Location SNMP on the list of services, then select it and click Stop.

Securiteam: [NT] Unchecked Buffer in SNMP Service Could Enable Arbitrary Code Execution

- * Select Startup, and click Disabled.
- * Click OK to close the dialogue, and then close the Computer Management window.

I have not installed the SNMP service on my system. Am I at any risk?
No. You are only at risk if the SNMP service is running.

ADDITIONAL INFORMATION

The information has been provided by <mailto:secure at MICROSOFT.COM>
Microsoft Security Response Center.

=====

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
In order to subscribe to the mailing list, simply forward this email to: 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: "[NEWS] Malformed Network Request can cause Office X for Mac to Fail"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)