

[NT] Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-07/msg00033.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 13 Jul 2006 01:17:27 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Vulnerability in Server Service Could Allow Remote Code Execution
(MS06-035)

SUMMARY

Improper handling of user input allows attackers to execute arbitrary code and retrieve information from Server Service.

DETAILS

Vulnerable Systems:

* Microsoft Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=b207020d-90f7-4c41-8304-06af0ded6467>>

Download the update

* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=2592a44c-82fb-4ccd-82a6-fcac7ca33172>>

Download the update

* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=b0f67167-7ede-4355-af6f-50c6615f6bbd>>

Download the update

* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

[NT] Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=48f03ad7-38f9-48f4-bbfc-14c52e9c942a>>

Download the update

* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=41a4a07f-bea3-48d6-b8d2-d7a5600d7179>>

Download the update

* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=dfbf3fa6-9e11-48b4-894d-5436693d17f7>>

Download the update

Immune Systems:

* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me)

Mailslot Heap Overflow Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1314>>

CVE-2006-1314:

There is a remote code execution vulnerability in the Server driver that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Mitigating Factors for Mailslot Heap Overflow Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1314>>

CVE-2006-1314:

* Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

* Microsoft Windows XP Service Pack 2 and Microsoft Windows Server 2003 Service Pack 1 do not have services listening on Mailslots in default configurations.

* Attempts to exploit this vulnerability will most probably result in a Denial of Service condition caused by an unexpected restart of the affected system rather than Remote Code Execution.

Workarounds for Mailslot Heap Overflow Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1314>>

CVE-2006-1314:

Microsoft has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

* Block TCP port 445 at the firewall:

This port is used to initiate a connection with the affected component. Blocking TCP port 445 at the firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports, visit the following

<<http://go.microsoft.com/fwlink/?LinkId=21312>> Web site.

* To help protect from network-based attempts to exploit this vulnerability, use a personal firewall, such as the <<http://go.microsoft.com/fwlink/?LinkId=33335>> Internet Connection Firewall, which is included with Windows XP and with Windows Server 2003.

By default, the Internet Connection Firewall feature in Windows XP and in Windows Server 2003 helps protect your Internet connection by blocking unsolicited incoming traffic. We recommend that you block all unsolicited incoming communication from the Internet. In Windows XP Service Pack 2 this feature is called the Windows Firewall.

To enable the Internet Connection Firewall feature by using the Network Setup Wizard, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Network and Internet Connections, and then click Setup or change your home or small office network. The Internet Connection Firewall feature is enabled when you select a configuration in the Network Setup Wizard that indicates that your system is connected directly to the Internet.

To configure Internet Connection Firewall manually for a connection, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Networking and Internet Connections, and then click Network Connections.
3. Right-click the connection on which you want to enable Internet Connection Firewall, and then click Properties.
4. Click the Advanced tab.
5. Click to select the Protect my computer or network by limiting or preventing access to this computer from the Internet check box, and then click OK.

Note If you want to enable certain programs and services to communicate through the firewall, click Settings on the Advanced tab, and then select the programs, the protocols, and the services that are required.

* To help protect from network-based attempts to exploit this vulnerability, enable advanced TCP/IP filtering on systems that support this feature.

You can enable advanced TCP/IP filtering to block all unsolicited inbound traffic. For more information about how to configure TCP/IP filtering, see <<http://support.microsoft.com/kb/309798>> Microsoft Knowledge Base Article 309798.

* To help protect from network-based attempts to exploit this vulnerability, block the affected ports by using IPSec on the affected

systems.

Use Internet Protocol security (IPSec) to help protect network communications. Detailed information about IPSec and about how to apply filters is available in <<http://support.microsoft.com/kb/313190>> Microsoft Knowledge Base Article 313190 and <<http://support.microsoft.com/kb/813878>> Microsoft Knowledge Base Article 813878.

FAQ for Mailslot Heap Overflow Vulnerability –
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1314>>
CVE-2006-1314:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

What causes the vulnerability?

An unchecked buffer in the Server service.

What is a Mailslot?

A mailslot is a temporary mechanism utilized by applications and processes to facilitate unidirectional data transfer. For more information about Mailslots, visit the following

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/base/writing_to_a_mailslot.asp> Web site.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

Who could exploit the vulnerability?

Any anonymous user who could deliver a specially crafted network packet to the affected system could try to exploit this vulnerability.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating and sending a specially crafted network packet to an affected system. The network packet could then cause the affected system to execute code.

What systems are primarily at risk from the vulnerability?

Workstations and servers are both at risk from this vulnerability.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the

[NT] Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035)

<<http://go.microsoft.com/fwlink/?LinkId=21169>> Protect Your PC Web site.
IT professionals can visit the
<<http://go.microsoft.com/fwlink/?LinkId=21171>> Security Guidance Center
Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Server driver validates the length of a message before it passes the message to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

SMB Information Disclosure Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1315>>
CVE-2006-1315:

There is an information disclosure vulnerability in the Server service that could allow an attacker to view fragments of memory used to store SMB traffic during transport.

Mitigating Factors for SMB Information Disclosure Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1315>>
CVE-2006-1315:

* Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

* For customers who require the affected component, firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

* On Windows 2000, Windows XP Service Pack 1, and Windows Server 2003, an attacker must have valid logon credentials to exploit this vulnerability. The vulnerability could not be exploited by anonymous users. However, the affected component is available remotely to users who have standard user accounts. In certain configurations, anonymous users could authenticate as the Guest account. For more information, see Microsoft Security Advisory 906574.

[NT] Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035)

* Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

Workarounds for SMB Information Disclosure Vulnerability –
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1315>>
CVE-2006-1315:

Microsoft has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

Note Other protocols such as Internetwork Packet Exchange (IPX) and Sequenced Packet Exchange (SPX) could be vulnerable to this issue. If vulnerable protocols such as IPX and SPX are in use, it is important to block the appropriate ports for those protocols as well. For more information about IPX and SPX, visit the following Microsoft
<http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prch_cnn_goue.asp>
Web site.

* Block TCP ports 139 and 445 at the firewall:

These ports are used to initiate a connection with the affected protocol. Blocking them at the firewall, both inbound and outbound, will help prevent systems that are behind that firewall from attempts to exploit this vulnerability. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports. For more information about ports, visit the following Web site.

* To help protect from network-based attempts to exploit this vulnerability, use a personal firewall, such as the
<<http://go.microsoft.com/fwlink/?LinkId=33335>> Internet Connection Firewall, which is included with Windows XP and with Windows Server 2003.

By default, the Internet Connection Firewall feature in Windows XP and in Windows Server 2003 helps protect your Internet connection by blocking unsolicited incoming traffic. We recommend that you block all unsolicited incoming communication from the Internet.

To enable the Internet Connection Firewall feature by using the Network Setup Wizard, follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Network and Internet Connections, and then click Setup or change your home or small office network. The Internet Connection Firewall feature is enabled when you select a configuration in the Network Setup Wizard that indicates that your system is connected directly to the Internet.

To configure Internet Connection Firewall manually for a connection,

[NT] Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035)

follow these steps:

1. Click Start, and then click Control Panel.
2. In the default Category View, click Networking and Internet Connections, and then click Network Connections.
3. Right-click the connection on which you want to enable Internet Connection Firewall, and then click Properties.
4. Click the Advanced tab.
5. Click to select the Protect my computer or network by limiting or preventing access to this computer from the Internet check box, and then click OK.

Note If you want to enable certain programs and services to communicate through the firewall, click Settings on the Advanced tab, and then select the programs, the protocols, and the services that are required.

* To help protect from network-based attempts to exploit this vulnerability, enable advanced TCP/IP filtering on systems that support this feature.

You can enable advanced TCP/IP filtering to block all unsolicited inbound traffic. For more information about how to configure TCP/IP filtering, see <http://support.microsoft.com/kb/309798> Microsoft Knowledge Base Article 309798.

To help protect from network-based attempts to exploit this vulnerability, block the affected ports by using IPsec on the affected systems.

Use Internet Protocol security (IPsec) to help protect network communications. Detailed information about IPsec and about how to apply filters is available in <http://support.microsoft.com/kb/313190> Microsoft Knowledge Base Article 313190 and <http://support.microsoft.com/kb/813878> Microsoft Knowledge Base Article 813878.

FAQ for SMB Information Disclosure Vulnerability –
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1315>
CVE-2006-1315:

What is the scope of the vulnerability?

This is an information disclosure vulnerability. An attacker who successfully exploited this vulnerability could remotely read information stored in buffers for Server Message Block traffic. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly. It could be used to produce useful information to try to further compromise the affected system.

What causes the vulnerability?

An uninitialized buffer in the Server protocol driver.

What is SMB?

Server Message Block (SMB), and its follow-on,

[NT] Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035)

<<http://www.microsoft.com/mind/1196/cifs.asp>> Common Internet File System (CIFS), is the Internet Standard protocol that Windows uses to share files, printers, serial ports, and also to communicate between computers. To do this, SMB uses named pipes and mail slots. In a networked environment, servers make file systems and resources available to clients. Clients make SMB requests for resources. Servers make SMB responses. This is described as a client server, request-response protocol.

Does this vulnerability also affect CIFS?

Common Internet File System (CIFS) is an Internet Standard protocol. The vulnerability described here resides specifically in Microsoft's implementation of the protocol and not the protocol itself.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could remotely view contents of the SMB buffers.

Who could exploit the vulnerability?

Any anonymous user who could deliver a specially crafted message to the affected system could try to exploit this vulnerability.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system. The attacker could then retrieve information in the SMB buffers.

What systems are primarily at risk from the vulnerability?

Both workstations and servers are at risk. Servers could be at more risk, especially if they support a large amount of SMB traffic.

Could the vulnerability be exploited over the Internet?

Yes. An attacker could try to exploit this vulnerability over the Internet. Firewall best practices and standard default firewall configurations can help protect against attacks that originate from the Internet. Microsoft has provided information about how you can help protect your PC. End users can visit the <<http://go.microsoft.com/fwlink/?LinkId=21169>> Protect Your PC Web site. IT professionals can visit the <<http://go.microsoft.com/fwlink/?LinkId=21171>> security Guidance Center Web site.

What does the update do?

The update removes the vulnerability by initializing the buffer prior to responding to a client request.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure.

When this security bulletin was issued, had Microsoft received any reports

[NT] Vulnerability in Server Service Could Allow Remote Code Execution (MS06-035)

that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS06-035.msp>>

<http://www.microsoft.com/technet/security/Bulletin/MS06-035.msp>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.