

# [NT] Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Could Allow Remote Code Execution (MS04-01)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0049.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/14/04

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

Date: 14 Jan 2004 11:13:31 +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 Microsoft Internet Security and Acceleration Server 2000  
H.323 Filter Could Allow Remote Code Execution (MS04-01)

---

## SUMMARY

A security vulnerability exists in the H.323 filter for Microsoft Internet Security and Acceleration Server 2000 that could allow an attacker to overflow a buffer in the Microsoft Firewall Service in Microsoft Internet Security and Acceleration Server 2000. An attacker who successfully exploited this vulnerability could try to run code of their choice in the security context of the Microsoft Firewall Service. This would give the attacker complete control over the system. The H.323 filter is enabled by default on servers running ISA Server 2000 computers that are installed in integrated or firewall mode.

## DETAILS

Affected Software:

\* Microsoft Internet Security and Acceleration Server 2000 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=CBE42990-4156-4E1D-9ACB-4CD449D9599B&dis>

Download the update

\* Microsoft Small Business Server 2000 (which includes Microsoft Internet

[NT] Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Could Allow Remote Code Execution

Security and Acceleration Server 2000) –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=CBE42990-4156-4E1D-9ACB-4CD449D9599B&discovery=source:msrp>

Download the update

\* Microsoft Small Business Server 2003 (which includes Microsoft Internet Security and Acceleration Server 2000) –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=CBE42990-4156-4E1D-9ACB-4CD449D9599B&discovery=source:msrp>

Download the update

Non Affected Software:

\* Microsoft Proxy Server 2.0

Mitigating factors:

\* ISA Servers running in cache mode are not vulnerable because the Microsoft Firewall Service is disabled by default

\* Users can prevent the risk of attack by disabling the H.323 filter

Workarounds:

Microsoft has tested the following workarounds. These workarounds will not correct the underlying vulnerability however, they help block known attack vectors. Workarounds may cause a reduction in functionality in some cases – in such situations this is identified below.

1. Disable the H.323 filter.

To disable the H.323 filter, follow these steps:

1. Open ISA management tool. Expand the Extensions container, expand the Application Filters container.
2. Select the H.323 Filter and then click Disable.
3. Restart the Microsoft Firewall Service Windows Components.

Impact of workaround:

If the H.323 filter is disabled, H.323 traffic is blocked by the Microsoft Firewall Service. This stops any applications that use the H.323 protocol for Internet Protocol (IP) telephony or data collaboration from communicating through the ISA Server. If H.323 traffic is not on the network with the ISA Server, disabling this filter and other unused filters is recommended for enhanced security and performance.

2. Block TCP port 1720 at a perimeter or gateway router.

By default, the H.323 filter listens on external Transmission Control Protocol (TCP) port 1720. Blocking this port at a perimeter router will help to protect the ISA Server from an Internet-based attack.

Note: Clicking to clear the Allow Incoming Calls check box on the Call Control tab of the H.323 filter settings does not configure the filter to stop listening on the external TCP port 1720 and is not an effective workaround. This behavior has been changed in this Security Update and is documented additionally in the "Frequently Asked Questions" section of this security bulletin.

Impact of workaround:

If port 1720 traffic is blocked, applications that use the H.323 protocol

for IP telephony or data collaboration can no longer be able to communicate over the Internet.

#### Frequently Asked Questions

What is the scope of the vulnerability?

This is a buffer overflow vulnerability. An attacker who successfully exploited this vulnerability could cause code to run in the security context of the Microsoft Firewall Service on ISA Server 2000. An attacker who successfully exploited this vulnerability could also gain complete control over the system.

What causes the vulnerability?

This vulnerability results because of the way that the H.323 filter checks the boundaries on specially crafted H.323 traffic.

What is the H.323 Filter?

The H.323 filter is an application filter that ISA Server 2000 uses to monitor and control traffic using H.323 and T.120 protocols. The H.323 protocol is used in IP telephony applications to transfer audio and video communications. The T.120 protocol is used in IP telephony applications to transfer data such as whiteboard, file transfer, or remote desktop data. The H.323 filter is enabled by default on ISA Server 2000.

What is the Microsoft Firewall Service?

ISA Server's Microsoft Firewall Service allows Internet applications to perform as if they were directly connected to the Internet. These services redirect the necessary communications functions to an ISA Server, establishing a communication path from the internal application to the Internet through the server computer.

The service eliminates the need for a specific gateway for each protocol, such as Simple Mail Transfer Protocol (SMTP), Telnet, File Transfer Protocol (FTP), or H.323 protocol.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause code to run in the security context of the Microsoft Firewall Service on ISA Server 2000. An attacker who successfully exploited this vulnerability could gain complete control over the system.

Does this update contain any other security changes?

Yes. The update also corrects an issue with the Call Control tab of the H.323 filter setting. Before this update if you clicked to clear the Allow Incoming Calls check box in the Call Control tab of the H.323 filter settings, the filter would not be configured to stop listening on the external TCP port 1720. This update corrects this problem. After the update, clicking to select this option correctly configures the filter to stop listening on the external TCP port 1720. The Microsoft Firewall Service must be restarted for this setting to take effect.

If the network that the H.323 filter is helping to protect intends to use only outgoing H.323 traffic, it is recommended that you disable Allow Incoming Calls to enhance security.

What does the update do?

The update removes the vulnerability by modifying the way that the H.323 filter validates H.323 traffic.

I have installed the H.323 Gatekeeper Service. Is the H.323 Gatekeeper Service vulnerable?

No. The H.323 Gatekeeper Service does not contain the vulnerability that is associated with this update. However, if the H.323 Gatekeeper Service has been installed on the system, an updated version of gksvc.dll will be installed with this update. The H.323 Gatekeeper Service is not installed by default.

If I install the H.323 Gatekeeper Service after I apply this update, do I need to re-apply the update?

Yes. If setup components are re-installed, all updates should be re-applied.

ADDITIONAL INFORMATION

The information has been provided by 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  
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.