

# [NT] IIS Redirection Remote Buffer Overflow Vulnerability (MS04-21)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0056.html>

---

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

**Date:** 07/14/04

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

Date: 14 Jul 2004 14:08:28 +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>

-----

IIS Redirection Remote Buffer Overflow Vulnerability (MS04-21)

---

## SUMMARY

A buffer overrun vulnerability exists in Internet Information Server 4.0 that could allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

## DETAILS

Vulnerable Systems:

\* Microsoft Windows NT Workstation 4.0 Service Pack 6a –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3A2B38C5-FA73-49EC-9EEF-06FE8D6495C0&dis>

Download the update

\* Microsoft Windows NT Server 4.0 Service Pack 6a –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3A2B38C5-FA73-49EC-9EEF-06FE8D6495C0&dis>

Download the update

Immune Systems:

\* Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4

## Securiteam: [NT] IIS Redirection Remote Buffer Overflow Vulnerability (MS04-21)

- \* Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- \* Microsoft Windows XP 64-Bit Edition Service Pack 1
- \* Microsoft Windows XP 64-Bit Edition Version 2003
- \* Microsoft Windows Server 2003
- \* Microsoft Windows Server 2003 64-Bit Edition
- \* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me)

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0205>>  
CAN-2004-0205

The vulnerability exists due to an unchecked buffer in the IIS redirection function. The redirection function can be used by an administrator to redirect an incoming request to a different directory or to another host. Successful exploitation of this remote vulnerability will allow arbitrary code execution on the target machine with the same privileges as the IIS server, typically SYSTEM.

### Mitigating Factors for IIS Redirection Vulnerability

- \* Internet Information Server 5.0, Internet Information Server 5.1, and Internet Information Server 6.0 are not affected by this vulnerability.
- \* Customers who have disabled permanent redirects are not at risk from this vulnerability.

### Workarounds for IIS Redirection Vulnerability

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

- \* Disable permanent redirects:
  - \* Open the IIS Configuration manager.
  - \* Right-click the Web site that you want to administer, and then click Properties.
  - \* Click Home Directory.
  - \* Uncheck A permanent redirection for this resource, and then click OK.

Impact of Workaround: The server will no longer perform redirects.

- \* Use URLScan to disallow the use of large requests
  - \* Visit the following Web site to  
<<http://www.microsoft.com/downloads/details.aspx?FamilyID=12244f33-a5da-4203-a3a8-83f4388bb71f&DisplayL>>  
Download and install the URLScan security tool.
  - \* Start Notepad, and then open the  
%systemroot%\winnt\urlscan\UrlScan.ini file.
  - \* Configure the MaxUrl setting so that it limits requests to 16 kilobytes (KB). To configure the MaxUrl setting to that it limits requests to 16 KB, add the following line to the RequestLimits section of the file:  
MaxUrl = 16384
  - \* Save, and then close the UrlsScan.ini file.

## Securiteam: [NT] IIS Redirection Remote Buffer Overflow Vulnerability (MS04-21)

\* Start, and then stop the World Wide Web Publishing Service by using the Services item in Control Panel. You can also do this by using the net stop IISadmin command and the net start w3svc command at a command prompt. For information about how to do this, see Microsoft Knowledge Base Article <<http://support.microsoft.com/default.aspx?scid=kb:en-us:185382>> 185382.

Impact of workaround: The URLScan tool will block all the incoming requests that are larger than 16 KB.

\* Reduce MaxClientRequestBuffer

- \* Start Registry Editor (Regedt32.exe).
- \* Locate the following key in the registry:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\w3svc\parameters
- \* Click Edit, click Add Value, and then add the following registry value:  
Value Name: MaxClientRequestBufferData Type: REG\_DWORD
- \* In the DWORD Editor dialog box, under Radix, click Decimal.
- \* In the Data box, type the number of bytes for the maximum URL request. Set the size so that it is equal to or less than 16384 bytes.

Note: You must restart the IIS service for the changes to take effect. For more information, see Microsoft Knowledge Base Article <<http://support.microsoft.com/default.aspx?scid=kb:en-us:260694>> 260694.

Impact of workaround: Any incoming request that is larger than 16384 bytes will fail.

- \* Stop, disable, or remove IIS
- \* You can stop the World Wide Web Publishing Service component of IIS by issuing the net stop w3svc command at a command prompt.
- \* You can use the IIS Manager to disable or stop IIS.
- \* You can stop or disable the World Wide Web Publishing Service by using the Services item in Control Panel.
- \* You can use Add or Remove Programs in Control Panel to remove IIS from your system. To find IIS, click Add/Remove Windows Components.

Impact of Workaround: If you stop the World Wide Web Publishing Service component of IIS, the system can no longer provide Web content. If you stop or remove IIS, the system can no longer provide Web, File Transfer Protocol (FTP), or NTP content. The Simple Mail Transfer Protocol (SMTP) service will also be unavailable.

### Frequently Asked Questions for IIS Redirection Vulnerability

What is the scope of the vulnerability ?

This is a buffer overrun vulnerability. An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

What causes the vulnerability ?

The vulnerability is caused by an unchecked buffer in the IIS 4.0 redirect

function.

What is a redirect ?

By using the IIS 4.0 redirect function, an administrator can forward incoming requests to another virtual directory or to another server.

Does the IIS Lockdown Tool block this attack ?

Yes. The IISLockdown tool installs URLScan, which can be used to block this attack. You must configure the URLScan tool by following the steps that are described in the Workarounds for IIS Redirection Vulnerability section of this bulletin to block this attack.

Will the URLScan tool block this attack ?

Yes. You can configure the URLScan tool to block this by following the steps that are described in the Workarounds for IIS Redirection Vulnerability section of this bulletin.

What is redirection ?

Redirection occurs when a Web browser makes a request for a Web page that does not exist, and the Web server redirects the browser to another page, such as to a generic error page or to the Web site's home page. For example, the Web page <http://microsoft.com/xp> does not exist, but instead of providing an error, the Web server redirects the browser to a page that suggests pages that the user may have been looking for and provides a site map. This process is redirection.

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 message to the affected system could exploit this vulnerability.

How could an attacker exploit the vulnerability ?

An attacker could exploit the vulnerability by creating a specially crafted message and sending the message to an affected system, which could then cause the affected system to execute code.

What systems are primarily at risk from the vulnerability ?

Systems that have Windows NT 4.0 and IIS 4.0 installed are at risk from this vulnerability. IIS 4.0 is available as part of the

<http://www.microsoft.com/downloads/details.aspx?FamilyID=05c301d2-51f6-4cc1-b750-02f3c3141a71&displayla>  
Windows NT 4.0 Server Option Pack.

Could the vulnerability be exploited over the Internet ?

Yes. An attacker could exploit this vulnerability over the Internet.

What does the update do ?

The update removes the vulnerability by modifying the way that IIS 4.0 validates the length of request before it passes the message to the

Securiteam: [NT] IIS Redirection Remote Buffer Overflow Vulnerability (MS04-21)

allocated buffer.

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

No. Microsoft had not received any information indicating that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

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

No. Microsoft had not received any information indicating 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.

Why is there no update available for Microsoft Windows NT Server 4.0 Terminal Server Edition ?

Windows NT 4.0 Option Pack is not supported on Microsoft Windows NT Server 4.0 Terminal Server Edition. For more information see Microsoft Knowledge Base Article <<http://support.microsoft.com/?kbid=190157>> 190157.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS04-021.msp>>  
<http://www.microsoft.com/technet/security/bulletin/MS04-021.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@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.