

[NT] Web Client Service Remote Code Execution (MS06-008)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00056.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2006 11:41:19 +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>

Web Client Service Remote Code Execution (MS06-008)

SUMMARY

A remote code execution vulnerability exists in the way that Windows processes Web Client requests. This could allow an attacker to take complete control of the affected system.

DETAILS

Vulnerable Systems:

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=62535040-5204-4469-B0BF-EAE14567C2D5>>

Download the update

* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9734F634-6869-434F-AAF0-47B70F84D178>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=FA073183-0C83-4F1C-BE46-A2EE8A1A1440>>

Download the update

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

[NT] Web Client Service Remote Code Execution (MS06-008)

Windows Server 2003 with SP1 for Itanium-based Systems

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E186E149-208A-4035-A0FC-E1CBDE4E6FEF>>

Download the update

* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=E2F5413A-0B77-4C18-9BAB-E2470D3D3F4E>>

Download the update

* Note The security updates for Microsoft Windows Server 2003, Microsoft Windows Server 2003 Service Pack 1, and Microsoft Windows Server 2003 x64 Edition also apply to Microsoft Windows Server 2003 R2.

Immune Systems:

* Microsoft Windows 2000 Service Pack 4

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

Mitigating Factors for Web Client Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0013>>

CVE-2006-0013:

* An attacker must have valid logon credentials to exploit this vulnerability. The vulnerability could not be exploited remotely 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

<<http://www.microsoft.com/technet/security/advisory/906574.mspx>> Microsoft Security Advisory 906574.

* By default, the Web Client service is disabled in Windows Server 2003 and Windows Server 2003 Service Pack 1. An administrator would have to manually enable this service for the system to become vulnerable to this issue.

* 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. By default, the Internet Connection Firewall that is provided as part of Windows XP Service Pack 1 and Windows Server 2003 blocks the affected ports from responding to network-based attempts to exploit this vulnerability.

Workarounds for Web Client Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0013>>

CVE-2006-0013:

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 in the following section.

Disable the Web Client service

[NT] Web Client Service Remote Code Execution (MS06-008)

Disabling the Web Client service will help protect the affected system from attempts to exploit this vulnerability. To disable the Web Client service, follow these steps:

1. Click Start, and then click Control Panel. Alternatively, point to Settings, and then click Control Panel.
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click WebClient.
5. In the Startup type list, click Disabled.
6. Click Stop, and then click OK.

You can also stop and disable the Web Client service by using the following command at the command prompt:

```
sc stop WebClient & sc config WebClient start= disabled
```

Impact of Workaround: If the Web Client service is disabled, Web Distributed Authoring and Versioning (WebDAV) requests are not transmitted. If the Web Client service is disabled, any services that explicitly depend on the Web Client service will not start, and an error message will be logged in the System log. Windows Server 2003 users will not be able to use the "Open as Web Folder" functionality.

Use the Group Policy settings to disable the WebClient service on all affected systems that do not require this feature.

Because the Web Client service is a possible attack vector, disable the service by using the Group Policy settings. You can disable the startup of this service at either the local, site, domain, or organizational-unit level by using Group Policy object functionality in Windows 2000 domain environments or in Windows Server 2003 domain environments.

Note You may also review the

<<http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx>> Windows Server 2003 Security Guide. This guide includes information about how to disable services.

For more information about Group Policy, visit the following Microsoft Web sites:

*

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep>> Step-by-Step Guide to Understanding the Group Policy Feature Set

*

<<http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp>> Windows 2000 Group Policy

*

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/default.mspx>> Group Policy in Windows Server 2003

Impact of Workaround: If the Web Client service is disabled, Web Distributed Authoring and Versioning (WebDAV) requests are not

[NT] Web Client Service Remote Code Execution (MS06-008)

transmitted. If the Web Client service is disabled, any services that explicitly depend on the Web Client service will not start, and an error message will be logged in the System log. Windows Server 2003 users will not be able to use the "Open as Web Folder" functionality.

Block TCP ports 139 and 445 at the firewall:

Although WebDAV uses TCP port 80 for outbound communication, TCP ports 139 and 445 can be used inbound to attempt to connect to this service and try to exploit this vulnerability. Blocking them at the firewall can 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. 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

[NT] Web Client Service Remote Code Execution (MS06-008)

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 Web Client Vulnerability –
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0013>>
CVE-2006-0013:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could 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. To attempt to exploit the vulnerability, an attacker must have valid logon credentials. The vulnerability could not be exploited by anonymous users. An attacker could also use this vulnerability to perform a local elevation of privilege attack.

What causes the vulnerability?

An unchecked buffer in the WebClient service.

What is the Web Client service?

The Web Client service allows applications to access documents on the Internet. Web Client extends the networking capability of Windows by allowing standard Win32 applications to create, read, and write files on Internet file servers by using the WebDAV protocol. The WebDAV protocol is a file-access protocol that is described in XML and that travels over the Hypertext Transfer Protocol (HTTP). By using standard HTTP, WebDAV runs over the existing Internet infrastructure. For example, WebDAV runs over firewalls and routers.

If the Web Client service is stopped, you will be prevented from using the Web Publishing Wizard to publish data to the Internet for locations that use the WebDAV protocol. If this service is disabled, any services that explicitly depend on this service will not start. For more information on WebDAV, see the following

[NT] Web Client Service Remote Code Execution (MS06-008)

<<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/844f5e01-4b9e-4dac-897e-2a0bb>> product documentation.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could 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.

Who could exploit the vulnerability?

To attempt to exploit the vulnerability, an attacker must have valid logon credentials. The vulnerability could not be exploited by anonymous users. Even though the Web Client service is used to support the WebDAV protocol over the Internet, an authenticated attacker must perform the steps that are required to attempt to exploit this issue. If the Guest account has been enabled on an affected system, then this attack could be performed by any user. For more information, see <<http://www.microsoft.com/technet/security/advisory/906574.msp>> Microsoft Security Advisory 906574.

How could an attacker exploit the vulnerability?

An attacker would first have to authenticate to the system. An attacker could then try to exploit the vulnerability directly over a network by creating a series of specially crafted messages and sending them to an affected system. The messages could then cause the affected system to execute code.

What systems are primarily at risk from the vulnerability?

All affected operating systems are at risk from this vulnerability. The Internet Connection Firewall that is provided as part of Windows XP Service Pack 1 and Windows Server 2003 blocks the affected ports from responding to network-based attempts to exploit this vulnerability. The Internet Connection Firewall is not enabled by default on Windows XP Service Pack 1. By default, the Web Client service is disabled in Windows Server 2003.

Note By default, exceptions will be automatically created after enabling File & Printer Sharing which allow access from the network. This access is limited to the local subnet by default.

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.

[NT] Web Client Service Remote Code Execution (MS06-008)

What does the update do?

The update removes the vulnerability by modifying the way that the Web Client service 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.

How does this vulnerability relate to the Web Client Vulnerability that is corrected by MS05-028?

Both vulnerabilities were in Web Client service. However, this update addresses a new vulnerability that was not addressed as part of MS05-028. MS05-028 helps protect against the vulnerability that is discussed in that bulletin, but does not address this new vulnerability. This update replaces MS05-028. You must install this update to help protect your system against both vulnerabilities.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<http://www.microsoft.com/technet/security/Bulletin/MS06-008.msp>

<http://www.microsoft.com/technet/security/Bulletin/MS06-008.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@xxxxxxxxxxxxxxx

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

=====

=====

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,

[NT] Web Client Service Remote Code Execution (MS06-008)

loss of business profits or special damages.