

[NT] Vulnerability in Remote Desktop Protocol Allows DoS (MS05-041)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0044.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/10/05

To: list@securiteam.com

Date: 10 Aug 2005 14:47:47 +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 Remote Desktop Protocol Allows DoS (MS05-041)

SUMMARY

A denial of service vulnerability exists that could allow an attacker to send a specially crafted Remote Data Protocol (RDP) message to an affected system. An attacker could cause this system to stop responding.

DETAILS

Affected Software:

* Microsoft Windows 2000 Server Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=18255896-8C5D-45C5-8840-C0C6EE1B14BB>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A229F193-DA3F-4014-925D-1EACF5BA296C>>

Download the update

* Microsoft Windows XP Professional x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=79AD267F-1A2E-4597-AFD6-53369F0DD8B7>>

Download the update

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

Securiteam: [NT] Vulnerability in Remote Desktop Protocol Allows DoS (MS05-041)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=EFD642EF-95E2-4A99-8FFD-6032D86282A2>>

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=E5342572-C494-489D-A69E-290070EBFF1C>>

Download the update

* Microsoft Windows Server 2003 x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=F3DBA966-0F24-4129-9B55-2144E7F9D5DA>>

Download the update

Non-Affected Software:

* Microsoft Windows 2000 Professional Service Pack 4

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

Microsoft Windows Millennium Edition (ME)

CVE Information:

Remote Desktop Protocol Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1218>>

CAN-2005-1218

Mitigating Factors for Remote Desktop Protocol Vulnerability –

CAN-2005-1218:

* 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 Remote Desktop Protocol (RDP) is not enabled on any operating system version. On Windows XP and Windows Server 2003, Remote Assistance can enable RDP. On Windows XP Media Center Edition, RDP is enabled if a Media Center Extender has been installed. For information about Media Center Extenders, visit the following

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/mcxwp/html/windows_media_center_extender_and
Web site.

On Small Business Server 2000 and on Windows Small Business Server 2003, RDP is enabled by default. However, by default, on Windows Small Business Server 2003 and earlier, the RDP Protocol communication ports are blocked from the Internet. RDP is available only on the local network unless Terminal Services or the Remote Web Workplace features have been enabled by using the Configure E-mail and Internet Connection Wizard (CEICW).

* If Remote Desktop is manually enabled, the following Windows Firewall changes will occur, depending on the operating system version:

* On Windows XP Service Pack 2 systems that have the Windows Firewall enabled, enabling the Remote Desktop feature will automatically enable the Remote Desktop exception in the firewall, with the scope of All computers (including those on the Internet). When you disable Remote Desktop, this firewall exception is automatically disabled.

On Windows XP Service Pack 1, Windows Server 2003, and Windows Server 2003 Service Pack 1, enabling the Remote Desktop Feature does not enable the

Securiteam: [NT] Vulnerability in Remote Desktop Protocol Allows DoS (MS05-041)

Remote Desktop exception in the firewall. Enabling Remote Desktop causes a dialog box that indicates that you must manually enable this exception. There is a Remote Desktop entry in the exception in the list of the firewall exceptions that a user would have to manually enable. Disabling Remote Desktop does not change the exception status in the firewall. However, although the system is no longer vulnerable to this issue through Remote Desktop, it could still be vulnerable through Remote Assistance and Terminal Services, where available.

Workarounds for Remote Desktop Protocol Vulnerability – CAN-2005-1218: 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 Terminal Services, Remote Desktop, Remote Assistance, and Windows Small Business Server 2003 Remote Web Workplace feature if they are no longer required.

If you no longer need these services on your system, consider disabling them as a security best practice. Disabling unused and unneeded services helps reduce your exposure to security vulnerabilities.

For information about how to disable Remote Desktop manually, visit the following

<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/rdesktop_disable.mspx> Web site.

For information about how to disable Remote Desktop by using Group Policy, see the following <<http://support.microsoft.com/kb/306300>> Microsoft Knowledge Base Article.

For information about Remote Assistance, including instructions on how to disable Remote Assistance manually and by using Group Policy, visit the following

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/intmgmt/20_xprem.mspx> Web site.

For information about how to disable the Windows Small Business Server 2003 Terminal Services and Remote Web Workplace features, visit the following

<http://www.microsoft.com/technet/security/secnews/articles/sec_sbs2003_network.mspx#EIAA> Web site.

* Block TCP port 3389 at the enterprise perimeter firewall:

This port is used to initiate a connection with the affected component. Blocking it at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability.

This can help protect networks from attacks that originate outside the enterprise perimeter. Blocking the affected ports at the enterprise perimeter is the best defense to help avoid Internet-based attacks.

However, systems could still be vulnerable to attacks from within their enterprise perimeter. Additionally, on Windows XP and Windows Server 2003, the Windows Firewall can help protect individual systems. By default, the Windows Firewall does not allow connections to this port, except in Windows XP Service Pack 2 when the Remote Desktop feature is enabled. For

Securiteam: [NT] Vulnerability in Remote Desktop Protocol Allows DoS (MS05-041)

information about how to disable the Windows Firewall exception for Remote Desktop on these platforms, visit the following

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/8b5e3b52-b77b-4d98-a058->

Web site. If you cannot disable the Windows Firewall exception for Remote Desktop, you may be able to reduce the scope of this vulnerability by setting the default value of All computers (Including those on the Internet), to the local network. Doing this helps reduce the likelihood of attacks from the Internet.

Note Windows Small Business Server 2003 uses a feature named Remote Web Workplace. This feature uses TCP port 4125 to listen for RDP connections.

If you are using this feature, you should validate that this port is also blocked from the Internet in addition to port 3389.

Note It is possible to manually change the affected components to use other ports. If you have performed these actions, you should also block those additional ports.

* Help secure Remote Desktop Connections by using an IPsec policy. Specific configurations would be dependent upon the individual environment. For information about Internet Protocol Security (IPsec), visit the following

<<http://www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.msp>> Web site.

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.

* Help secure Remote Desktop Connections by using a virtual private network (VPN) connection.

Specific configurations depend on the individual environment. For information about Virtual Private Networks, visit the following

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/a08da8ea-a616-4422-bbd7->

FAQ for Remote Desktop Protocol Vulnerability – CAN-2005-1218:

What is the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who exploited this vulnerability could cause the affected system to stop responding and automatically restart. During that time, the server could not respond to requests. The denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests.

What causes the vulnerability?

The process used to validate data by the Remote Desktop Protocol.

What is Remote Desktop Protocol (RDP)?

Remote Desktop Protocol (RDP) lets users create a virtual session on their desktop computers. It allows remote users to access all the data and applications on their computers. For more information about RDP, visit the following

<http://msdn.microsoft.com/library/en-us/termserv/termserv/remote_desktop_protocol.asp> Web site.

In which Microsoft products is RDP implemented?

In general, RDP is the underlying protocol for Windows features that allow remote desktop sessions. These features include:

Securiteam: [NT] Vulnerability in Remote Desktop Protocol Allows DoS (MS05-041)

* Terminal Services in Windows 2000 and in Windows Server 2003 implement RDP. For more information about Terminal Services and RDP, visit the following

<<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/termserv/default.mspx>> Web site.

* Remote Desktop in Windows XP implements RDP. For more information about the Remote Desktop feature in Windows XP, visit the following

<http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/pree_rem_higy.asp> Web site.

* Creating a Remote Assistance request in Windows XP and Windows Server 2003 enables RDP until a short time after the request expires. For information about Remote Assistance, including instructions on how to disable Remote Assistance manually and by using Group Policy, visit the following

<http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/intmgmt/20_xprem.mspx> Web site.

* Media Center Extenders on Windows XP Media Center Edition 2005 systems enable RDP. For information about Media Center Extenders, visit the following

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/mcxwp/html/windows_media_center_extender_and> Web site. For detailed technical information about Media Center Extenders, visit the following

<<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/MedctrSDK/htm/mediacenterextenders.asp>>

Web site. The Media Center Extenders can use RDP over ports beyond the default TCP 3389 port.

* Remote Web Workplace in Windows Small Business Server 2003 enables RDP.

For more information about this feature, see the following

<<http://support.microsoft.com/kb/833983>> TechNet Support WebCast. For information about how to disable the Windows Small Business Server 2003 Remote Web Workplace feature, visit the following

<http://www.microsoft.com/technet/security/secnews/articles/sec_sbs2003_network.mspx#EIAA> Web site.

The Remote Web Workplace feature will use RDP over ports beyond the default TCP 3389 port.

Is RDP enabled by default in Windows?

No. By default, the Remote Desktop Protocol (RDP) is not enabled on any operating system version. On some versions of Windows XP Media Center Edition, RDP is enabled if a Media Center Extender has been installed. For information about Media Center Extenders, visit the following

<<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/MedctrSDK/htm/mediacenterextenders.asp>>

Web site. For detailed technical information about Media Center Extenders, visit the following

<<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/MedctrSDK/htm/mediacenterextenders.asp>>

Web site.

Small Business Server 2000 and Windows Small Business Server 2003 enable RDP by default. However, by default, on Windows Small Business Server 2003 and earlier, the RDP Protocol communication ports are blocked from the Internet and RDP is available only on the local network, unless Terminal Services or Remote Web Workplace has been enabled by using the Configure E-mail and Internet Connection Wizard (CEICW).

Windows XP Home Edition does not support Remote Desktop. However, it does support Remote Assistance. Remote Assistance enables RDP until a short time after the Remote Assistance request expires. During this time, Windows XP Home systems could be vulnerable to this issue if they allow the Remote Desktop exception through the Windows Firewall.

What might an attacker use the vulnerability to do?

Securiteam: [NT] Vulnerability in Remote Desktop Protocol Allows DoS (MS05-041)

An attacker who exploited this vulnerability could cause the affected system to stop responding.

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. Receipt of such a message could cause the vulnerable system to fail in such a way that it could cause a denial of service.

What systems are primarily at risk from the vulnerability?

Windows 2000 Server-based terminal servers and Windows Server 2003-based terminal servers are primarily at risk from this vulnerability.

Administrators must manually configure these operating system versions to enable the Terminal Server features to become vulnerable to this issue.

Windows Small Business Server 2003-based servers are also at risk if the administrator has used the Configure E-mail and Internet Connection Wizard to enable Terminal Services or the Remote Web Workplace connections to the server from the Internet. Windows XP and Windows Server 2003 systems are at risk if they have manually enabled Remote Desktop or are using Remote Assistance. Windows 2000 Professional does not contain support for the RDP protocol and is not vulnerable to this issue.

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 modifying the way that RDP validates the length of a message before reading the message.

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

Yes. This vulnerability has been publicly disclosed.

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.

Does applying this security update help protect customers from the vulnerability details that had been published publicly?

Yes. This security update addresses the vulnerability details that have

Securiteam: [NT] Vulnerability in Remote Desktop Protocol Allows DoS (MS05-041)

been published on this issue.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-041.msp>>

<http://www.microsoft.com/technet/security/Bulletin/MS05-041.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.