

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

[NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0040.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 10/13/04

To: list@securiteam.com

Date: 13 Oct 2004 16:05:57 +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 NetDDE Could Allow Remote Code Execution (MS04-031)

SUMMARY

A remote code execution vulnerability exists in the NetDDE services because of an unchecked buffer. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, the NetDDE services are not started by default and would have to be manually started for an attacker to attempt to remotely exploit this vulnerability. This vulnerability could also be used to attempt to perform a local elevation of privilege or remote denial of service.

DETAILS

Affected Software:

* Microsoft Windows NT Server 4.0 Service Pack 6a

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A5CA71B6-8A5E-4AA9-B34E-7CE5B304CFAC>>

Download the update

* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0A584B37-291C-4B63-971E-FB35CC361B13>>

Download the update

* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=80FE311A-B446-43D0-9614-B93112E28294>>

Download the update

* Microsoft Windows XP and Microsoft Windows XP Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C6EB8FB6-6AAE-48BC-9E4F-271F81361AE0>>

Download the update

* Microsoft Windows XP 64-Bit Edition Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7754DB47-5D9E-4652-8634-ECF7B9D6786C>>

Download the update

* Microsoft Windows XP 64-Bit Edition Version 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0C73C1B4-0E12-49F9-BAB7-606B07BFF569>>

Download the update

* Microsoft Windows Server 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=01CFA2F4-19B2-4771-8377-FB633C5BF464>>

Download the update

* Microsoft Windows Server 2003 64-Bit Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0C73C1B4-0E12-49F9-BAB7-606B07BFF569>>

Download the update

* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) Review the FAQ section of this bulletin for details about these operating systems.

Non-Affected Software:

* Microsoft Windows XP Service Pack 2

The software in this list has been tested to determine if the versions are affected. Other versions either no longer include security update support or may not be affected. To determine the support lifecycle for your product and version, visit the following

<<http://go.microsoft.com/fwlink/?LinkId=21742>> Microsoft Support Lifecycle Web site.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0206>>
CAN-2004-0206

Frequently asked questions (FAQ) related to this security update:

I am still using Windows XP, but extended security update support ended on September 30th, 2004. However, this bulletin has a security update for this operating system version. Why is that?

The original version of Windows XP, commonly known as Windows XP Gold or Windows XP Release to Manufacturing (RTM) version, reached the end of its extended security update support life cycle on September 30, 2004.

However, the end-of-life occurred very recently. In this case, the majority of the steps that are required to address this vulnerability were completed before this date. Therefore, we have decided to release a security update for this operating system version as part of this security bulletin.

We do not anticipate doing this for future vulnerabilities that may affect this operating system version, but we reserve the right to produce updates and to make these updates available when necessary. It should be a

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

priority for customers who have this operating system version to migrate to supported operating system versions to prevent potential exposure to vulnerabilities. For more information about the Windows Service Pack Product Life Cycle, visit the Microsoft Support Lifecycle Web site. For more information about the Windows Product Life Cycle, visit the Microsoft Support Lifecycle Web site.

I am still using Microsoft Windows NT 4.0 Workstation Service Pack 6a or Windows 2000 Service Pack 2, but extended security update support ended on June 30, 2004. What should I do?

Windows NT 4.0 Workstation Service Pack 6a and Windows 2000 Service Pack 2 have reached the end of their life cycles as previously documented, and Microsoft extended this support to June 30, 2004.

It should be a priority for customers who have these operating system versions to migrate to supported versions to prevent potential exposure to vulnerabilities. For more information about the Windows Product Life Cycle, visit the following <<http://go.microsoft.com/fwlink/?LinkId=21742>> Microsoft Support Lifecycle Web site. For more information about the extended security update support period for these operating system versions, visit the Microsoft Product Support Services Web site.

I am still using Microsoft Windows NT 4.0 Workstation Service Pack 6a or Windows 2000 Service Pack 2, but extended security update support ended on June 30, 2004. What should I do?

Windows NT 4.0 Workstation Service Pack 6a and Windows 2000 Service Pack 2 have reached the end of their life cycles as previously documented, and Microsoft extended this support to June 30, 2004.

It should be a priority for customers who have these operating system versions to migrate to supported versions to prevent potential exposure to vulnerabilities. For more information about the Windows Product Life Cycle, visit the following <<http://go.microsoft.com/fwlink/?LinkId=21742>> Microsoft Support Lifecycle Web site. For more information about the extended security update support period for these operating system versions, visit the <<http://go.microsoft.com/fwlink/?LinkId=21742>> Microsoft Product Support Services Web site.

Customers who require additional support for Windows NT Workstation 4.0 SP6a must contact their Microsoft account team representative, their Technical Account Manager, or the appropriate Microsoft partner representative for custom support options. Customers without an Alliance, Premier, or Authorized Contract can contact their local Microsoft sales office. For contact information, visit the Microsoft Worldwide Information Web site, select the country, and then click Go to see a list of phone numbers. When you call, ask to speak with the local Premier Support sales manager.

For more information, visit the <<http://go.microsoft.com/fwlink/?LinkId=33330>> Windows Operating System FAQ.

How does the extended support for Windows 98, Windows 98 Second Edition, and Windows Millennium Edition affect the release of security updates for

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

these operating systems?

Microsoft will only release security updates for critical security issues. Non-critical security issues are not offered during this support period. For more information about the Microsoft Support Lifecycle policies for these operating systems, visit the following

<<http://support.microsoft.com/default.aspx?pr=LifeAn1>> Web site.

For more information about severity ratings, visit the following

<<http://go.microsoft.com/fwlink/?LinkId=21140>> Web site.

Are Windows 98, Windows 98 Second Edition, or Windows Millennium Edition critically affected by the vulnerability that is addressed in this security bulletin?

No. This vulnerability is not critical in severity on Windows 98, on Windows 98 Second Edition, or on Windows Millennium Edition.

Can I use the Microsoft Baseline Security Analyzer (MBSA) to determine if this update is required?

Yes. MBSA will determine if this update is required. For more information about MBSA, visit the <<http://go.microsoft.com/fwlink/?LinkId=21134>> MBSA Web site.

Note After April 20, 2004, the Mssecure.xml file that is used by MBSA

1.1.1 and earlier versions is no longer being updated with new security bulletin data. Therefore, scans that are performed after that date with MBSA 1.1.1 or earlier will be incomplete. All users should upgrade to MBSA 1.2 because it provides more accurate security update detection and supports additional products. Users can download MBSA 1.2 from the <<http://go.microsoft.com/fwlink/?LinkId=21134>> MBSA Web site. For more information about MBSA support, visit the following <<http://www.microsoft.com/technet/security/tools/mbsaqa.msp>> Microsoft Baseline Security Analyzer 1.2 Q&A Web site.

Can I use Systems Management Server (SMS) to determine if this update is required?

Yes. SMS can help detect and deploy this security update. For information about SMS, visit the <<http://go.microsoft.com/fwlink/?LinkId=21158>> SMS Web site.

Mitigating Factors for NetDDE Vulnerability:

- * 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 Server 2003 the NetDDE services are disabled by default. Typically only administrators can change the startup type of a service. An attacker would first have to change the startup type from Disabled, and then start the service to attempt to exploit this vulnerability.

- * Disabling the NetDDE services helps prevent the possibility of a remote attack. See the Workarounds section for instructions that describe how to disable these services. Operating systems other than Windows Server 2003

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

have the NetDDE services startup type set to Manual instead of Disabled by default.

*

<<http://www.microsoft.com/technet/Security/prodtech/win2000/secwin2k/06basewn.mspx>> Chapter 6 of the Microsoft Solution for Securing Windows 2000 Server, Hardening the Base Windows 2000 Server recommends disabling the NetDDE services. Environments that comply with these guidelines could be at a reduced risk from this vulnerability.

Workarounds for NetDDE 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 the NetDDE services:

Disabling the NetDDE services will help protect from remote attempts to exploit this vulnerability. You can disable the NetDDE services by following these steps:

1. Click Start, and then click Control Panel (or point to Settings, and then click Control Panel).
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click Network DDE.
5. In the Startup type list, click Disabled.
6. Click Stop, and then click OK.
7. Double-click Network DDE DSDM.
8. In the Startup type list, click Disabled.
9. Click Stop, and then click OK.

Impact of Workaround: If the NetDDE services are disabled, messages from NetDDE applications are not transmitted. If the NetDDE services are disabled, any services that explicitly depend on the NetDDE services will not start, and an error message is logged in the system event log.

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

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

Note You may also review the

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&Di>> Windows 2000 Hardening Guide. This guide includes information about how to disable services.

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

*

<<http://www.microsoft.com/windows2000/techinfo/planning/management/groupsteps.asp>> 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

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

*

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

Impact of Workaround: If the NetDDE services are disabled, messages from NetDDE applications are not transmitted. If the NetDDE services are disabled, any services that explicitly depend on the NetDDE services will not start, and an error message is logged in the system event log.

Block the following at the firewall:

- * UDP ports 135, 137, 138, and 445, and TCP ports 135, 139, 445, and 593
- * All unsolicited inbound traffic on ports greater than 1024
- * Any other specifically configured RPC port

These ports can be used to initiate a connection to an affected system. Blocking them at the firewall will help prevent systems that are behind that firewall from attempts to exploit this vulnerability. Also, make sure that you block any other specifically configured RPC port on the remote system. 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 the ports that RPC uses, visit the following <<http://go.microsoft.com/fwlink/?LinkId=21312>> Web site.

Use a personal firewall such as the

<<http://www.microsoft.com/security/protect/windowsxp/firewall.asp>>
Internet Connection Firewall, which is included with Windows XP and Windows Server 2003.

If you use the Internet Connection Firewall feature in Windows XP or in Windows Server 2003 to help protect your Internet connection, it blocks unsolicited inbound traffic by default. We recommend blocking all unsolicited inbound communication from the Internet.

Note This procedure does not apply to Windows XP Service Pack 2. Windows XP Server Pack 2 is not affected by this vulnerability.

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

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

preventing access to this computer from the Internet check box, and then click OK.

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

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 Microsoft Knowledge Base Article <<http://support.microsoft.com/default.aspx?scid=kb:en-us:309798>> 309798.

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 how to apply filters is available in Microsoft Knowledge Base Articles <<http://support.microsoft.com/default.aspx?scid=kb:en-us:313190>> 313190 and <<http://support.microsoft.com/?id=813878>> 813878.

FAQ for NetDDE Vulnerability:

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, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. However, the NetDDE services are not started by default and would have to be manually started for an attacker to attempt to remotely exploit this vulnerability. This vulnerability could also be used to attempt to perform a local elevation of privilege or remote denial of service.

What causes the vulnerability?

An unchecked buffer in the NetDDE services.

What is Network Dynamic Data Exchange?

Network Dynamic Data Exchange (NetDDE) allows two applications to communicate with each other over a network. This is considered an older communication method that typically has been replaced by newer technologies such as DCOM. For more information about DCOM, visit the <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomtec.asp> DCOM MSDN Web Site.

What applications or services require NetDDE?

NetDDE is considered to be an older network communication method. Applications such as the Windows for Workgroups 3.11 version of Microsoft Hearts (MSHearts) and Microsoft Chat (MSChat) application use NetDDE services. The version of Microsoft Hearts that is provided as part of Windows XP does not use NetDDE Services. The Clipbook service that is used to share a local clipboard to other systems in a network and the DDE Share Manager (DDEShare) application both require the NetDDE services. There are

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

cases when Microsoft Excel could also use NetDDE. Microsoft Knowledge Base Article <<http://support.microsoft.com/default.aspx?scid=kb:en-us:128491>> 128941 discusses how Microsoft Excel can use NetDDE. Third-party applications may also require the NetDDE services; therefore it is important to test the suggested workarounds in your organization before you deploy this update.

How can an administrator determine if NetDDE services are running?
Administrators can determine if the NetDDE services are running by viewing, Administrative Tools, Services, and searching for the NetDDE and the NetDDE DSDM services. The status of Started indicates that the services are running. See the Workarounds section of this security bulletin for instructions that explain how you can disable these services.

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?
After the NetDDE services are started, any anonymous user who could deliver a specially crafted message to the affected system could attempt to remotely exploit this vulnerability. Operating systems other than Windows XP Service Pack2 and Windows Server 2003 have the NetDDE services set to a startup type of Manual instead of Disabled. This could allow non privileged users to start the NetDDE services or could allow them to start an application that starts the NetDDE services. After the NetDDE services are started, the affected system could be vulnerable to a remote attack. To help prevent this, see the Workaround section for instructions that explain how you can disable the NetDDE services. This vulnerability could also be used to attempt to perform a local elevation of privilege.

How could an attacker exploit the vulnerability?
After a NetDDE service is started, 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 remotely execute code. Receipt of such a message could also cause the vulnerable system to fail in such a way that it could cause a denial of service.

To exploit this vulnerability for a local elevation of privilege, an attacker would first have to log on to the system. An attacker could then run a specially-designed application that could attempt to exploit the vulnerability and thereby gain complete control over the affected system.

An attacker could also access the affected component through another vector. For example, an attacker could use another program that passes parameters to the vulnerable component (locally or remotely).

What systems are primarily at risk from the vulnerability?
Workstations and terminal servers are primarily at risk. Servers are only at risk if users are given the ability to log on and to run programs.

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

However, best practices strongly discourage allowing this.

Windows XP Service Pack 2 is not vulnerable to this issue. Windows Server 2003 is impacted at a lower severity rating because the NetDDE services startup type is set to Disabled. An attacker would first have to change the setting from Disabled to Manual or Automatic, and then start the service to attempt to remotely exploit this vulnerability. Typically, only administrators can change the startup type of a service. Operating systems other than Windows Server 2003 have the NetDDE services set to a startup type of Manual instead of Disabled. This could allow non privileged users to start the NetDDE services or allow them to start an application that starts the NetDDE services. Once the NetDDE services are started the affected system could be vulnerable to a remote attack. To help prevent this, see the Workarounds section for instructions that explain how you can disable the NetDDE services.

Are Windows 98, Windows 98 Second Edition or Windows Millennium Edition critically affected by this vulnerability?

No. Although Windows 98, Windows 98 Second Edition, and Windows Millennium Edition do contain the affected component, the vulnerability is not critical because the NetDDE service is not started by default. For more information about severity ratings, visit the following <http://go.microsoft.com/fwlink/?LinkId=21140> Web site.

Could the vulnerability be exploited over the Internet?

Yes. If you have manually started the NetDDE services, or if you are using applications that may have started the NetDDE services, an attacker could attempt to remotely 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 the NetDDE services validate 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. 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

Securiteam: [NT] Vulnerability in NetDDE Could Allow Remote Code Execution (MS04-031)

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 Product Security.

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/MS04-031.msp>

<http://www.microsoft.com/technet/security/bulletin/MS04-031.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.