

[NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0040.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/15/04

To: list@securiteam.com

Date: 15 Sep 2004 11:21:47 +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>

Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

SUMMARY

This update resolves a newly-discovered, privately reported vulnerability. A buffer overrun vulnerability exists in the processing of JPEG image formats that could allow remote code execution on an affected system.

If a user is logged on with administrator privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

DETAILS

Vulnerable Systems:

* Microsoft Windows XP and Microsoft Windows XP Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=6F8D70C1-63BD-4213-82C1-20266FDFD735&disp>

Download the update

* Microsoft Windows XP 64-Bit Edition Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1631C3F7-A40E-4B26-BD92-12141E6A7F58&disp>

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

Download the update

* Microsoft Windows XP 64-Bit Edition Version 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=98BFF681-9703-4D23-8DF8-B7239D6C531C&disp>

Download the update

* Microsoft Windows Server 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B2FBD93C-3DC3-4A9E-BDD6-9F39726EE3E2&d>

Download the update

* Microsoft Windows Server 2003 64-Bit Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=98BFF681-9703-4D23-8DF8-B7239D6C531C&disp>

Download the update

* Microsoft Office XP Service Pack 3

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7D128614-6D34-49DF-8D63-6C17E9A2D312&disp>

Download the update

Microsoft Office XP Service Pack 3 Software:

* Outlook 2002

* Word 2002

* Excel 2002

* PowerPoint 2002

* FrontPage 2002

* Publisher 2002

* Microsoft Office 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=106BCF99-1BA9-4035-94C5-2A7FA90E5971&disp>

Download the update

Microsoft Office 2003 Software:

* Outlook 2003

* Word 2003

* Excel 2003

* PowerPoint 2003

* FrontPage 2003

* Publisher 2003

* InfoPath 2003

* OneNote 2003

* Microsoft Project 2002 Service Pack 1 (all versions)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B3EBCCEA-B0E4-41C7-A6F4-413864D2CCF3&d>

Download the update

* Microsoft Project 2003 (all versions)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9E37B6B0-A028-47EA-8FA1-3705877A2908&disp>

Download the update

* Microsoft Visio 2002 Service Pack 2 (all versions)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=16C2DFFD-7B73-43C4-AB0D-2B5EFC80EB63&d>

Download the update

* Microsoft Visio 2003 (all versions)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C07D40A5-6F87-4D50-9640-34FFD2F189E1&disp>

Download the update

* Microsoft Visual Studio .NET 2002

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=44004D19-B22F-4AF2-A701-1FCB0467F9&disp>

Download the update

Microsoft Visual Studio .NET 2002 Software:

* Visual Basic .NET Standard 2002

* Visual C# .NET Standard 2002

* Visual C++ .NET Standard 2002

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

* Microsoft Visual Studio .NET 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A13B7A21-463C-4286-AD68-E692417E80E2&dis>

Download the update

Microsoft Visual Studio .NET 2003 Software:

* Visual Basic .NET Standard 2003

* Visual C# .NET Standard 2003

* Visual C++ .NET Standard 2003

* Visual J# .NET Standard 2003

* The Microsoft .NET Framework version 1.0 SDK Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?familyid=6978D761-4A92-4106-A9BC-83E78D4ABC5B&dis>

Download the update

* Microsoft Picture It! 2002 (all versions)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&dis>

Download the update

* Microsoft Greetings 2002

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&dis>

Download the update

* Microsoft Picture It! version 7.0 (all versions)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&dis>

Download the update

* Microsoft Digital Image Pro version 7.0

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&dis>

Download the update

* Microsoft Picture It! version 9 (all versions, including Picture It!

Library)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&dis>

Download the update

* Microsoft Digital Image Pro version 9

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&dis>

Download the update

* Microsoft Digital Image Suite version 9

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B52-A344-502E25AAD7FE&dis>

Download the update

* Microsoft Producer for Microsoft Office PowerPoint (all versions)

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=1b3c76d5-fc75-4f99-94bc-784919468e73&DisplayI>

Download the update

* Microsoft Platform SDK Redistributable: GDI+ -

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=6A63AB9C-DF12-4D41-933C-BE590FEAA05A&d>

Download the update

Office Users Note An administrative update is also available for Office XP

(applicable to Service Pack 2 and Service Pack 3) and Office 2003; for

more information, see the Security Update Information section.

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9C51D3A6-7CB1-4F61-837E-5F938254FC47&dis>

Office 2003 Service Pack 1,

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=AFCA0578-E1FB-4540-B0CC-FF83DEF61CC6&di>

Visio 2003 Service Pack 1, and

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1B04C073-E58F-4F42-B76D-6B565A45CDC3&dis>

Project 2003 Service Pack 1 contain an updated version of the affected component and are not affected.

Customers that have installed these service packs do not need to install the available security updates for these products.

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

MSN 9 Users Note MSN 9 distributes Picture It! Express version 9 and Picture It! Library. You have the option to install these programs when you install MSN 9. You should install the Picture It! version 9 update only if you installed Picture It! Express version 9 or Picture It! Library when you installed MSN 9.

Affected Components:

- * Internet Explorer 6 Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B0095851-674D-4357-868C-DD75D88405EC&disp>>

Download the update

- * The Microsoft .NET Framework version 1.0 Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?familyid=6978D761-4A92-4106-A9BC-83E78D4ABC5B&disp>>

Download the update

- * The Microsoft .NET Framework version 1.1

<<http://www.microsoft.com/downloads/details.aspx?familyid=A8F5654F-088E-40B2-BBDB-A83353618B38&disp>>

Download the update

Immune Systems:

- * Microsoft Windows NT Server 4.0 Service Pack 6a
- * Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- * Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows XP Service Pack 2
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me)
- * Microsoft Office 2003 Service Pack 1
- * Microsoft Office 2000
- * Microsoft Visio 2003 Service Pack 1
- * Microsoft Visio 2000
- * Microsoft Project 2003 Service Pack 1
- * Microsoft Project 2000
- * Microsoft Digital Image Suite 10, Microsoft Digital Image Pro 10, Picture It! Premium 10

Non-Affected Components:

- * Internet Explorer 5.01 Service Pack 3 on Windows 2000 Service Pack 3
- * Internet Explorer 5.01 Service Pack 4 on Windows 2000 Service Pack 4
- * Internet Explorer 5.5 Service Pack 2 on Microsoft Windows Millennium Edition
- * The Microsoft .NET Framework version 1.0 Service Pack 3
- * The Microsoft .NET Framework version 1.1 Service Pack 1
- * The Microsoft .NET Framework version 1.1 Service Pack 1 for Windows Server 2003

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0200>>
CAN-2004-0200

Frequently asked questions (FAQ):

Why are there several affected programs and components?

Windows XP, Windows XP Service Pack 1, and Windows Server 2003 provide an

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

operating system version of the component that is vulnerable to this issue. Earlier versions of Windows did not provide an operating system version of this component. Therefore, when you install programs that require this functionality on earlier versions of Windows, this component is commonly installed. Typically, when these programs are installed on Windows XP, Windows XP Service Pack 1, or Windows Server 2003 they only use the version that is provided by the operating system, even if they install a copy of the vulnerable component.

The exceptions to this are Office XP, Visio 2002, Project 2002, Office 2003, Visio 2003, and Project 2003. To make sure that JPEG images are processed consistently across all operating systems, these programs use their own version of the vulnerable component. This version of the vulnerable component is installed on all operating systems that are supported by these programs. If you have installed these programs, you must install the update for these programs. You must also install an operating system update if you use Windows XP, Windows XP Service Pack 1, or Windows Server 2003.

Microsoft has created a tool that will also assist in detecting if you are running one or more affected products and components. Where can I get more information about this tool?

Microsoft has created the GDI+ Detection tool to assist customers in detecting if they are running one or more affected products that contain a vulnerable version of the JPEG Parsing component on their system.

Microsoft Knowledge Base Article

<http://support.microsoft.com/default.aspx?scid=kb;EN-US:873374> 873374 describes this tool as well as provides instructions on how to download this tool.

What does the GDI+ Detection tool do?

The GDI+ Detection tool scans your system for non-operating system products that are known to contain the vulnerable component. It then directs consumers to the appropriate locations for downloading an update to address the vulnerability.

Will the GDI+ Detection tool tell me if my system is at risk from this vulnerability?

No. The tool is only designed to scan the system and detect for certain installed products that are known to contain the vulnerable component. The tool is not able to determine if these products have already been updated to use a secure version of the affected component.

What is GDI+?

GDI+ is a graphics device interface that provides two-dimensional vector graphics, imaging, and typography to applications and programmers.

If I use Windows XP Service Pack 2 and use any of the affected software, what should I do?

Windows XP Service Pack 2 does not contain a vulnerable version of the

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

affected component. However, if you have installed any of the affected Office, Visio, or Project applications you should install the updates for those applications. The easiest way to address this vulnerability is to install the updates provided by

<<http://go.microsoft.com/fwlink/?LinkId=21135>> Office Update. If you have not installed any of the affected Office, Visio, or Project applications you do not have to install any other security updates because the other affected software and affected components use the operating system version of the vulnerable component on Windows XP Service Pack 2.

The exception for this is if you use Visual Studio .NET 2002 or Visual Studio .NET 2003 to develop applications that redistribute the Gdiplus.dll file. In this case you need to install the security updates for those programs even if you are using Windows XP Service Pack 2. See the Security Update Information section for these updates for more information.

If I use Windows XP, Windows XP Service Pack 1, or Windows Server 2003 and use any of the affected software, what should I do?

If you have installed any of the affected Office, Visio, or Project applications the easiest way to address this vulnerability is to install the updates provided by both <<http://go.microsoft.com/fwlink/?LinkId=21130>> Windows Update and <<http://go.microsoft.com/fwlink/?LinkId=21135>> Office Update. If you have not installed any of the affected Office, Visio, or Project applications the easiest way to address this vulnerability is to install the updates provided by Windows Update. You do not have to install any other security updates because the other affected software and affected components use the operating system version of the vulnerable component on Windows XP, Windows XP Service Pack 1, and Windows Server 2003.

The exception for this is if you use Visual Studio .NET 2002 or Visual Studio .NET 2003 to develop applications that redistribute the Gdiplus.dll file. In this case you need to install the security updates for those programs as well as the security update for Windows XP, Windows XP Service Pack 1, or Windows Server 2003. See the Security Update Information Sections for these updates for more information.

If I use Windows 98, Windows 98 Second Edition (SE), Windows Millennium Edition (Me), Windows NT 4.0, or Windows 2000, what should I do?

By default, these operating systems do not natively provide a version of the vulnerable component and are not affected. However, the vulnerable component is installed on these non-affected operating systems when you install any of the software programs or components that are listed in the Affected Software and Affected Components sections of this bulletin.

If you have installed any of the affected programs or components, you should install the required security updates for those programs or components. For example, if you have Internet Explorer 6 Service Pack 1 and Office XP installed on your Windows 2000 system, you have to install the Internet Explorer 6 Service Pack 1 security update and the Office XP security update. If you have not installed any of the affected programs or

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

components, you do not have to install any security updates.

If I use versions of Internet Explorer that are earlier than Internet Explorer 6 Service Pack 1, am I vulnerable to this issue?

Internet Explorer 5.01 Service Pack 3, Internet Explorer 5.01 Service Pack 4 on Windows 2000, and Internet Explorer 5.5 Service Pack 2 on Windows Me have been tested and they are not vulnerable.

Internet Explorer 6 is only supported when using Windows XP, Windows XP Service Pack 1, and Windows Server 2003. Internet Explorer 6 on Windows XP, Windows XP Service Pack 1, and Windows Server 2003 uses the operating system version of the vulnerable component. When the Windows XP, Windows XP Service Pack 1, and Windows Server 2003 operating system update is installed, Internet Explorer 6 is not vulnerable. Windows XP Service Pack 2 includes Internet Explorer 6 Service Pack 2 and is not vulnerable to this issue. Internet Explorer 6 is no longer in support on other operating systems and may be vulnerable to this issue on those operating systems. Customers who do not use Windows XP, Windows XP Service Pack 1, or Windows Server 2003 and who use versions of Internet Explorer 6 that are earlier than Internet Explorer 6 Service Pack 1 should upgrade to Internet Explorer 6 Service Pack 1 and then install the Internet Explorer 6 Service Pack 1 security update provided in this security bulletin, or upgrade to <http://www.microsoft.com/windowsxp/sp2/default.mspx> Windows XP Service Pack 2 for Windows XP customers. To install Internet Explorer 6 Service Pack 1, visit the following <http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/default.asp> Web site. For more information about the support lifecycle for Internet Explorer, visit the following <http://go.microsoft.com/fwlink/?LinkId=21742> Microsoft Support Lifecycle Web site.

If use Visual Studio .NET 2002, Visual Studio .NET 2003, the Microsoft NET Framework 1.0 SDK Service Pack 2, or the Microsoft Platform SDK Redistributable: GDI+ to develop applications, what should I do? When these programs are installed on Windows XP, Windows XP Service Pack 1, or Windows Server 2003 they use the operating system version of the vulnerable component. If you are using these programs on Windows XP, Windows XP Service Pack 1, or Windows Server 2003 make sure that you install the operating system version of the security update. If you are using these programs on other operating systems make sure that you install the update for these programs.

However, if you use these programs to create applications that distribute a version of the Gdiplus.dll file you need to install the appropriate security update based on the development tool you use, even if you have installed the Windows XP, Windows XP Service Pack 1, or Windows Server 2003 security update, or are using Windows XP Service Pack 2. If you use the Gdiplus.dll file for JPEG processing you should rebuild and redistribute your application using the updated version of the Gdiplus.dll file. For more information, see the appropriate Security Update Information sections depending on the developer tool you use.

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

Why is the fix for .NET Framework in a Service Pack?

This issue does not affect customers who have already deployed Microsoft .NET Framework 1.0 Service Pack 3 (SP3) and Microsoft .NET Framework 1.1 Service Pack 1 (SP1). These service packs, released prior to the release of this security bulletin, already contain the fix for this issue as well as other security changes for all reported customer issues found after the release of these software components. Therefore, we highly recommended that customers using .NET Framework 1.0 or 1.1 install these Service Packs for increased security not only for this vulnerability but also for all reported customer issues found after the release of the Microsoft .NET Framework.

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

Yes. MBSA does detect if the update for this vulnerability is required for Office XP, Office 2003, Project 2002, Project 2003, Visio 2002, and Visio 2003. However, MBSA does not currently support the detection of several of the programs that are listed in the Affected Software and Affected Components section of this security bulletin. For detailed information about the programs that MBSA currently does not detect, see Microsoft Knowledge Base Article

<<http://support.microsoft.com/default.aspx?scid=kb;en-us;306460>> 306460.

If you have installed any of the programs that are listed in the Affected Software and Affected Components section of this security bulletin you may have to manually determine if you have to install the required update. For example, a Windows 2000 or Windows NT 4.0 system that has installed Internet Explorer 6 Service Pack 1 will need to install the Internet Explorer 6 Service Pack 1 security update and MBSA will not detect the missing update in these configurations. Also, MBSA cannot use the Office Detection Tool to scan remote systems, it will only use this tool to scan a system locally for required security updates. 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 <<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. SMS uses MBSA for detection; therefore, SMS has the same limitation listed earlier in this bulletin related to programs that MBSA

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

does not detect. However, SMS can also use the Microsoft Office Inventory Tool to detect for required updates for Microsoft Office components.

Can I use SMS to determine if programs are installed that have to be updated?

Yes. SMS can help detect if any of the affected programs or affected components are installed that may have installed a version of the vulnerable component. SMS can search for the existence of the file Gdiplus.dll. For the affected programs and components listed in this bulletin you need to update all versions of Gdiplus.dll that are earlier than version 5.1.3102.1355. See the Could I still be vulnerable even after I have installed all required security updates? FAQ earlier in this bulletin for more information about other applications that may have installed the Gdiplus.dll file.

Installations of Office XP, Visio 2002, Project 2002, and Internet Explorer 6 Service Pack 1 (SP1) combine the features of the vulnerable component with other files. For Office XP and Project 2002 you would also have to search for the existence of the Mso.dll file. Update all versions of Mso.dll that are earlier than version 10.0.6714.0. For Visio 2002, you have to search for the existence of the Mso.dll file and the Gdiplus.dll file because Visio 2002 distributes both files, except on Windows XP, or Windows Server 2003 where it only distributes the Mso.dll file.

For installations of Internet Explorer 6 Service Pack 1 that are not running on the Windows XP or Windows Server 2003 operating systems, search for the Vgx.dll file. Update all versions of Vgx.dll that are earlier than version 6.0.2800.1411. Internet Explorer 6 Service Pack 1 uses the operating system version of the vulnerable component on Windows XP and Windows Server 2003. You do not have to update Internet Explorer 6 Service Pack 1 for those operating systems. These .dll files are documented in the Security Update Information section of this security bulletin. You can also deploy the updates provided in this bulletin using the <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/patchupdate.msp> Inventory and Software Distribution feature of SMS.

I use Software Update Services (SUS) to deploy security updates in my enterprise. Should I deploy the GDI+ Detection Tool to all of my systems? While it is possible to deploy the GDI+ Detection Tool via SUS to all of the systems in an enterprise, it is not recommended or supported. The GDI+ Detection Tool will direct end users back to the Microsoft Windows Update site to scan their machines for updates.

What security updates will Windows Update offer to help address this vulnerability?

Windows Update will offer the required operating system updates for Windows XP, Windows XP Service Pack 1, and Windows Server 2003. Windows XP Service Pack 2 does not require an update because it does not contain a vulnerable version of the affected component. Windows Update will offer the Internet Explorer 6 Service Pack 1 security update to Windows 98, Windows 98 SE, Windows Me, Windows NT 4.0 and Windows 2000 operating

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

systems. Windows Update will offer the .NET Framework, version 1.0 Service Pack 2 (SP2) and the .NET Framework, version 1.1 Service Pack 1 to Windows NT 4.0 and Windows 2000 operating systems. These security updates are not offered to Windows XP or Windows Server 2003 systems because these components use the operating system version of the component on Windows XP and Windows Server 2003.

What security updates will Office Update offer to help address this vulnerability?

Office Update will offer the required updates for Office XP, Office 2003, Project 2002, Project 2003, Visio 2002, and Visio 2003. These security updates are required on all operating systems where these products are installed. Office 2003 Service Pack 1, Visio 2003 Service Pack 1, and Project 2003 Service Pack 1 are not affected and will be offered to customers using Office 2003, Project 2003, and Visio 2003 instead of the individual updates. Customers who have installed these service packs are not affected by this vulnerability from these applications.

What security updates will not be offered through Windows Update or Office Update to help address this vulnerability and should be manually installed?

Windows Update and Office Update do not provide support for the remaining programs. This includes the security updates for Visual Studio .NET 2002 (and all included programs), Visual Studio .NET 2003 (and all included programs), Greetings 2002, Picture It! (all versions), Digital Image (all versions), the Microsoft .NET Framework version 1.0 SDK Service Pack 2, Producer for Microsoft Office PowerPoint (all versions), and the Platform SDK Redistributable: GDI+. These security updates are required on Windows 98, Windows 98 SE, Windows Me, Windows NT 4.0 and Windows 2000 operating systems where these products are installed. Note Visual Studio .NET 2002 Enterprise Architect and Visual Studio .NET 2003 Enterprise Architect include Visio 2002. Visio 2002 is supported by Office Update.

Could I still be vulnerable even after I have installed all required security updates?

Yes. There are cases in which you might be vulnerable to this issue even after you install the required operating system update and the updates for programs or components that are listed in the Affected Software and Affected Components sections of this bulletin. The following examples document some of the possible cases:

* You may have installed a third-party program that has installed the affected component. If the Gdiplus.dll file is installed on your system, you may have to install an update for that program. It is possible that not every program that installs this file is vulnerable to this issue because it may not use the Gdiplus.dll file to process JPEG images. However, only the manufacturer of that program can make that determination. This could include third party applications that were developed using Visual Studio .NET 2002, Visual Studio .NET 2003, or the Microsoft .NET Framework 1.0 SDK Service Pack 2. Typically, even if the affected component is installed on a system that is running Windows XP or

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

Windows Server 2003, the program still uses the operating system version of the affected component.

* On Windows XP or Windows Server 2003, it is possible for a developer or administrator to force a program to bypass the vulnerable operating system component and instead use a version that they supply. This feature is not likely to be used in most circumstances. You may want to consider contacting the third-party application manufacturer for an updated version of their program, if they verify that their program uses this bypass feature. Steps to determine if you are using such a program are located in Microsoft Knowledge Base Article [835322](http://support.microsoft.com/default.aspx?scid=kb:en-us:835322).

In these cases, you would only be vulnerable to this issue while using the affected program to process images. Installing the operating system update and the updates for the affected programs and components listed in this bulletin will help reduce the chance that you will be attacked from the most common attack vectors an attacker could use to exploit this vulnerability.

Mitigating factors for JPEG Vulnerability:

* An attacker who successfully exploited this vulnerability could gain the same privileges as the user. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

* The vulnerability could only be exploited by an attacker who persuaded a user to open a specially crafted file or to view a directory that contains the specially crafted image. There is no way for an attacker to force a user to open a malicious file.

* In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.

* Windows XP, Windows XP Service Pack 1, and Windows Server 2003 are the only operating systems that contain the vulnerable component by default. By default, Windows 98, Windows 98 SE, Windows Me, Windows NT 4.0, and Windows 2000 are not. However, the vulnerable component will be installed by any of the programs listed in the affected software section of this bulletin on these operating systems and you should install the appropriate security update for those programs.

* Windows XP Service Pack 2 is not affected by this vulnerability.

Workarounds for JPEG 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.

Read e-mail messages in plain text format if you are using Outlook 2002 or later, or Outlook Express 6 SP1 or later, to help protect yourself from

the HTML e-mail attack vector.

Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or later and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about enabling this setting in Outlook 2002, see Microsoft Knowledge Base Article

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:307594>> 307594.

For information about this setting in Outlook Express 6, see Microsoft Knowledge Base Article <<http://support.microsoft.com/?kbid=291387>> 291387.

Impact of Workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. Additionally:

- * The changes are applied to the preview pane and to open messages.
- * Pictures become attachments so that they are not lost. Note Manually viewing these pictures could allow remote code execution if you are using a vulnerable application or operating system.
- * Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

FAQ for JPEG Vulnerability:

What is the scope of the vulnerability?

This is a buffer overrun vulnerability. If a user is logged on with administrator privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

What causes the vulnerability?

An unchecked buffer in the processing of JPEG images.

What are JPEG images?

JPEG is a platform-independent image format that supports a high level of compression. JPEG is a widely supported Internet standard developed by the Joint Photographic Experts Group.

What might an attacker use the vulnerability to do?

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

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

How could an attacker exploit this vulnerability?

Any program that processes JPEG images could be vulnerable to this attack.

Here are some examples:

- * An attacker could host a malicious Web site that is designed to exploit this vulnerability through Internet Explorer 6 and then persuade a user to view the Web site.

- * An attacker could also create an HTML e-mail message that has a specially crafted image attached. The specially crafted image could be designed to exploit this vulnerability through Outlook 2002 or Outlook Express 6. An attacker could persuade the user to view or preview the HTML e-mail message.

- * An attacker could embed a specially crafted image in an Office document and then persuade the user to view the document.

- * An attacker could add a specially crafted image to the local file system or onto a network share and then persuade the user to preview the directory by using Windows Explorer.

What systems are primarily at risk from the vulnerability?

The vulnerability could only be exploited on the affected systems by an attacker who persuaded a user to open a specially crafted file or view a directory that contains the specially crafted image. There is no way for an attacker to force a user to open a malicious file.

In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.

Windows XP, Windows XP Service Pack 1, and Windows Server 2003 are vulnerable by default. Windows XP Service Pack 2, Windows 98, Windows 98 SE, Windows Me, Windows NT 4.0, and Windows 2000 are not vulnerable by default. However, the vulnerable component could be installed by any of the products listed in the affected software section on these operating systems. Third-party applications that perform JPEG processing; third-party applications that were developed using Visual Studio .NET 2002, Visual Studio .NET 2003, or the Microsoft .NET Framework version 1.0 SDK Service Pack 2; and third-party applications that distribute their own copy of the vulnerable component may be also vulnerable.

What does the update do?

The update removes the vulnerability by modifying the way that Windows validates the affected image types.

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.

Securiteam: [NT] Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028)

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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@microsoft.com>
Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms04-028.msp>>

<http://www.microsoft.com/technet/security/bulletin/ms04-028.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.