

MinorRev: Microsoft Security Bulletin MS04-028 – Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-09/0065.html>

From: Russ Cooper (*Russ.Cooper_at_TRUSECURE.CA*)

Date: 09/27/04

Date: Mon, 27 Sep 2004 13:54:00 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS04-028:

Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)

Bulletin URL:

<<http://www.microsoft.com/technet/security/bulletin/MS04-028.msp>>

Reason for Revision: Affected and Non-Affected Software Sections updated. Updated Security Update Information Sections for Office XP, Visio 2002, Project 2002, .NET Framework 1.0 and .NET Framework 1.1. FAQ's have also been updated to provide additional information about this issue.

Version Number: 1.2

Issued Date: Tuesday, September 14, 2004

Revision Date: Tuesday, September 21, 2004

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Patch(es) Replaced: None

Caveats: If you have installed any of the affected programs or affected components listed in this bulletin, you should install the required security update for each of the affected programs or affected components. This may require the installation of multiple security updates. See the FAQ section of this bulletin for more information.

Tested Software:

Affected Software:

* Microsoft Windows XP and Microsoft Windows XP Service Pack 1

<<http://tinyurl.com/4fmzh>>

* Microsoft Windows XP 64-Bit Edition Service Pack 1

<<http://tinyurl.com/4zg68>>

* Microsoft Windows XP 64-Bit Edition Version 2003

<<http://tinyurl.com/6arva>>

* Microsoft Windows Server(tm) 2003

<<http://tinyurl.com/43too>>

* Microsoft Windows Server 2003 64-Bit Edition

<<http://tinyurl.com/6arva>>

* Microsoft Office XP Service Pack 3

<<http://tinyurl.com/64orn>>

MinorRev: Microsoft Security Bulletin MS04-028 – Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution

* Microsoft Office XP Service Pack 2 Microsoft Office XP Software:

- Outlook. 2002
- Word 2002
- Excel 2002
- PowerPoint. 2002
- FrontPage. 2002
- Publisher 2002
- Access 2002

<<http://tinyurl.com/5t8gq>>

* Microsoft Office 2003 Microsoft Office 2003 Software:

- Outlook. 2003
- Word 2003
- Excel 2003
- PowerPoint. 2003
- FrontPage. 2003
- Publisher 2003
- Access 2003
- InfoPath(tm) 2003
- OneNote(tm) 2003

<<http://tinyurl.com/58zvm>>

* Microsoft Project 2002 (all versions) and Microsoft Project 2002 Service Pack 1 (all versions)

<<http://tinyurl.com/7xuno>>

* Microsoft Project 2003 (all versions)

<<http://tinyurl.com/5ba7j>>

* Microsoft Visio 2002 Service Pack 1 (all versions) and Microsoft Visio 2002 Service Pack 2 (all versions)

<<http://tinyurl.com/67g3k>>

* Microsoft Visio 2003 (all versions)

<<http://tinyurl.com/4xhuy>>

* Microsoft Visual Studio .NET 2002 Microsoft Visual Studio .NET 2002 Software:

- Visual Basic .NET Standard 2002
- Visual C# .NET Standard 2002
- Visual C++ .NET Standard 2002

<<http://tinyurl.com/5ptm3>>

* Microsoft Visual Studio .NET 2003 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

<<http://tinyurl.com/4tnq2>>

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

<<http://tinyurl.com/5qet2>>

* Microsoft Picture It!. 2002 (all versions)

<<http://tinyurl.com/3q869>>

* Microsoft Greetings 2002

<<http://tinyurl.com/3q869>>

* Microsoft Picture It! version 7.0 (all versions)

<<http://tinyurl.com/3q869>>

* Microsoft Digital Image Pro version 7.0

<<http://tinyurl.com/3q869>>

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

<<http://tinyurl.com/3q869>>

- * Microsoft Digital Image Pro version 9
<<http://tinyurl.com/3q869>>
- * Microsoft Digital Image Suite version 9
<<http://tinyurl.com/3q869>>
- * Microsoft Producer for Microsoft Office PowerPoint (all versions)
<<http://tinyurl.com/4u9xy>>
- * Microsoft Platform SDK Redistributable: GDI+
<<http://tinyurl.com/3qqd8>>

Affected Components:

- * Internet Explorer 6 Service Pack 1
<<http://tinyurl.com/5zjvb>>
- * The Microsoft .NET Framework version 1.0 Service Pack 2
<<http://tinyurl.com/5qet2>>
- * The Microsoft .NET Framework version 1.1
<<http://tinyurl.com/5j55a>>

Technical Description:

* JPEG Vulnerability – CAN-2004-0200: A buffer overrun vulnerability exists in the processing of JPEG image formats that could allow remote code execution on an affected system. Any program that processes JPEG images on the affected systems could be vulnerable to this attack, and any system that uses the affected programs or components could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Revision History:

- * v1.0 – 9/14/2004: Bulletin published
- * v1.1 – 9/15/2004: Affected and Non-Affected Software Sections updated. Office XP Service Pack 2 is affected and this has been clarified. The .NET Framework 1.1 SDK and MS Works (all versions) are not affected and have been added to the Non Affected Software Section. FAQ's have also been updated to provide additional information about this issue.
- * v1.2 – 9/21/2004: Affected and Non-Affected Software Sections updated. Updated Security Update Information Sections for Office XP, Visio 2002, Project 2002, .NET Framework 1.0 and .NET Framework 1.1. FAQ's have also been updated to provide additional information about this issue.

This email is sent to NTBugtraq automatically as a service to my subscribers. (v4.01.1664.40858)

Cheers,
Russ – Senior Scientist – TruSecure Corporation/NTBugtraq Editor

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.