

Security Advisory August 15, 2007

Microsoft released 9 security bulletins this month. Additional attention should be paid to the advisory number MS07-046 - Vulnerability in GDI Could Allow Remote Code Execution as it is rated high risk for the State and Local government by the Multi-State Sharing and Analysis Center (MS-ISAC).

KB #	Exploit Type	Principle type of systems exposed	Exploit details public? / Being exploited?	Comprehensive, practical workaround available?	MS severity rating	Vulnerable Windows or Office versions				Notes	Randy's recommendation
	Product					2000	XP	2003	Vista/2007		
MS07-042 - 936227	Arbitrary code Windows, XML Core Services	Workstations & Terminal Servers	No/No	No	Critical	Yes	Yes	Yes	Yes	XML Core Services may get installed by MS apps in addition to Windows. See KB269238	Patch after testing
MS07-043 - 921503	Arbitrary code Windows, Visual Basic, Office for Mac	Workstations & Terminal Servers	No/No	No	Critical	Yes	Yes	Yes	No	OLE Automation. Known issue for Visual Basic developers (KB921503) and users of 3 rd party developed VB apps (KB921503)	Patch after testing. Check 3 rd party apps. Developers, alert your users.
MS07-044 - 940965	Arbitrary code Office, Excel	Workstations & Terminal Servers	No/No	Yes	Critical	Yes	Yes	Yes	No		Patch after testing or use Office File Block policy workaround
MS07-045 - 937143	Arbitrary code, DOS Windows Internet Explorer	Workstations & Terminal Servers	No/No	No	Critical	Yes	Yes	Yes	Yes	Cumulative Update includes non-security fixes. Known issue in KB937143. Sets kill bits for several non-MS ActiveX controls	Patch after testing
MS07-046 - 938829	Arbitrary code Windows	Workstations & Terminal Servers	No/No	No	Critical	Yes	Yes	No if SP2	No	W2003 SP2 not affected	Patch after testing
MS07-047 - 936782	Arbitrary code Windows	Workstations & Terminal Servers	No/No	Yes	MS says Important; I say Critical	Yes	Yes	Yes	Yes	Windows Media Player skins. Known issue with .SWF Flash	Patch after testing or implement WMZ/WMD

										files (KB936782)	workaround
MS07-048 - 938123	Arbitrary code Windows	Workstations	No/No	Yes	MS says Important; I say Critical	No	No	No	Yes	Vista Gadgets	Patch after testing or use one of the workarounds supported by group policy
MS07-049 - 937986	Arbitrary code Virtual PC Virtual Server	Virtual PC & Virtual Server	No/No	No	MS says Important; I say Critical	Versions PRIOR to Virtual PC 2007 and Virtual PC Server 2005 R2 SP2					Install patch or upgrade to latest version
MS07-050 - 938127	Arbitrary code Windows, Internet Explorer	Workstations & Terminal Servers	No/No	Yes	Critical	Yes	Yes	Yes	Yes	Disable Vector Markup Language	Patch after testing or implement workaround

*- provided by ultimatewindowssecurity.com

SUBJECT: MS07-046

New Vulnerability in GDI Could Allow for Remote Code Execution

OVERVIEW:

A new vulnerability has been discovered in the components of Microsoft Windows that render images for the user. This vulnerability can be exploited if a user opens an email attachment containing a malicious image file. This vulnerability may affect any program that render images and successful exploitation may result in the attacker taking complete control of the affected system.

SYSTEMS AFFECTED:

- Microsoft Windows 2000 Service Pack 4
- **Microsoft Windows XP Service Pack 2**
- Microsoft Windows XP Professional x64 Edition
- Windows Server 2003 Service Pack 1
- Windows Server 2003 x64 Edition
- Windows Server 2003 Service Pack 1 for Itanium-based Systems

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: **High**

DESCRIPTION:

Microsoft Windows Graphic Rendering Engine fails to properly handle specially crafted image files. The Microsoft Windows graphic device interface (GDI) enables various applications to access devices that render images for the user on desktop displays and printers. GDI is installed by default on all Microsoft Windows Operating systems. This vulnerability may affect other programs installed on the local machine that use GDI, and could become possible attack vectors.

Exploitation of this vulnerability occurs when a user opens a maliciously crafted image file. Microsoft has confirmed that this vulnerability can be exploited if the user opens a malicious email attachment. Upon successful exploitation, the attacker could run arbitrary code in the context of the locally logged-in user. This could also allow the attacker to install programs, add, view or delete user data, or create new accounts on the system to attack the machine at a later date.

At this time there is no known publicly available exploit code or malicious files.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the appropriate patches to vulnerable systems as soon as possible, after appropriate testing.
- Run all software as a non-privileged user (one without administrative privilege) to diminish the effects of a successful attack.
- Do not open email attachments from un-trusted sources.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/ms07-046.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3034>

SecurityFocus:

<http://www.securityfocus.com/bid/25302>

US-CERT

<http://www.kb.cert.org/vuls/id/640136>