

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[Request Tracker for Windows \(WinRT\) by SecureScout v3.0.16 alpha](#) - Download Free WinRT v3.0.16 alpha installer by filling our download form. Size: 33MB

Download Here:

http://www.netvigilance.com/productdownloads?productname=winrt_setup_3_0_16

This Week in Review

Cloud computing and the law. New ISO standard for health information. CIS to release guidelines for measuring security. The feds enforcing HIPAA.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

• Health information security standard issued

In an effort to help protect personal health care information, the International Organization for Standardization (ISO) has published a new standard that specifies controls for managing health information security and utilizing best practices.

This new standard, announced in late August, addresses the use of internet and wireless technologies to share personal medical information, and the need to better protect confidentiality and keep data private.

Richard Rushing, CSO at wireless security firm AirDefense, told SCMagazineUS.com on Wednesday that the standard shows that many organizations have the same issues and that similar guidelines should be followed.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Health-information-security-standard-issued/article/116516/>

• Group to release uniform metrics to measure IT security

September 8, 2008 (IDG News Service) The Center for Internet Security (CIS) is set to release guidelines that enterprises can use to measure the state of their security, and it's also preparing to launch a service to help companies compare their security performance with that of their peers.

"The problem that we've come to recognize is that information security professionals really are growing more confused on how to define success," Miuccio said. "They know that compliance with regulatory requirements, and audit frameworks do not necessarily result in improved security and are not the best measures of success."

Every security professional has different definitions of how to evaluate organizational security, Miuccio said. To try to find common ground, CIS assembled 85 information security experts who will work together to identify uniform ways to measure eight different metrics. The metrics should be released in late October or early November, Miuccio said.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114260&source=rss_topic1

• Feds finally put teeth into HIPAA enforcement

September 8, 2008 (Computerworld) A data security audit that the U.S. Department of Health and Human Services conducted at Piedmont Hospital in Atlanta last year was widely viewed within the health care industry as a harbinger of further actions by the federal government to enforce HIPAA's security and privacy rules.

On July 15, Providence agreed to adopt a so-called corrective action plan (CAP) and pay \$100,000 to settle what HHS described as "potential violations" of the Health Insurance Portability and Accountability Act's requirements for safeguarding electronic patient data.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=325376&source=rss_topic17

• Open phones are more vulnerable, security execs say

September 12, 2008 (Computerworld) SAN FRANCISCO -- The opening up of the mobile industry is great news for application developers but not so good for IT security professionals who want to sleep at night, executives from the security industry said yesterday.

"Everyone has now decided that the developers are very important for the future of this business. If a developer can load software on a device, a hacker can load software on a device," said Mark Kominsky, CEO of Bluefire Security Technologies, during a panel discussion at the CTIA Wireless I.T. & Entertainment show. "I think we're probably 12 to 18 months away from something big happening," he added.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114582&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 16474 Wireshark TCP dissector Denial of Service Vulnerability (Remote File Checking)

packet-tcp.c in the TCP dissector in Wireshark (formerly Ethereal) 0.99.2 through 0.99.4 allows remote attackers to cause a denial of service (application crash or hang) via fragmented HTTP packets.

The vulnerabilities are reported in versions 0.99.2 to 0.99.4.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack** Risk: **Medium**

References:

* MISC:

http://bugs.wireshark.org/bugzilla/show_bug.cgi?id=1200

* CONFIRM:

<http://www.wireshark.org/security/wnpa-sec-2007-01.html>

* CONFIRM:

<https://issues.rpath.com/browse/RPL-985>

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2007-166.htm>

* MANDRIVA: MDKSA-2007:033

<http://www.mandriva.com/security/advisories?name=MDKSA-2007:033>

* REDHAT: RHSA-2007:0066

<http://www.redhat.com/support/errata/RHSA-2007-0066.html>

* SGI: 20070301-01-P

<ftp://patches.sgi.com/support/free/security/advisories/20070301-01-P.asc>

* BID: 22352

<http://www.securityfocus.com/bid/22352>

* FRSIRT: ADV-2007-0443

<http://www.frsirt.com/english/advisories/2007/0443>

* SECTRACK: 1017581

<http://securitytracker.com/id?1017581>

* SECUNIA: 24016

<http://secunia.com/advisories/24016>

* SECUNIA: 24011

<http://secunia.com/advisories/24011>

* SECUNIA: 24025

<http://secunia.com/advisories/24025>

* SECUNIA: 24084

<http://secunia.com/advisories/24084>

* SECUNIA: 24515

<http://secunia.com/advisories/24515>

* SECUNIA: 24650

<http://secunia.com/advisories/24650>

* SECUNIA: 24970

<http://secunia.com/advisories/24970>

* XF: wireshark-tcpdissector-dos(32053)

<http://xforce.iss.net/xforce/xfdb/32053>

CVE Reference:

CVE-2007-0459 (cve.mitre.org, nvd.nist.gov)

• 18082 VMware Server, ActiveX control unspecified vulnerability (CVE-2007-5438) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in Reconfig.DLL in VMware Server before 1.0.7 build 108231, might allow local users to cause a denial of service to the Virtual Disk Mount Service (vmount2.exe), related to the ConnectPopulatedDiskEx function.

The issue is fixed in VMware Server 1.0.7.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Low**

References:

* BUGTRAQ: 20071010 [ELEYTT] 10PAZDZIERNIK2007

<http://www.securityfocus.com/archive/1/archive/1/482021/100/0/threaded>

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* MISC:

http://www.eleytt.com/advisories/eleytt_VMWARE1.pdf

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 26025
<http://www.securityfocus.com/bid/26025>
* FRSIRT: ADV-2008-2466
<http://www.frsirt.com/english/advisories/2008/2466>
* SECUNIA: 31707
<http://secunia.com/advisories/31707>
* SECUNIA: 31708
<http://secunia.com/advisories/31708>
* SECUNIA: 31709
<http://secunia.com/advisories/31709>
* SECUNIA: 31710
<http://secunia.com/advisories/31710>
* SREASON: 3219
<http://securityreason.com/securityalert/3219>

CVE Reference:

CVE-2007-5438 (cve.mitre.org, nvd.nist.gov)

• 18097 Windows Media Player Sampling Rate Vulnerability (MS08-054/954154) (Remote File Checking)

A remote code execution vulnerability exists in Windows Media Player 11. An attacker could exploit the vulnerability by constructing a specially crafted audio file that could allow remote code execution when streamed from a Windows Media server using Windows Media Player 11. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-054
<http://www.microsoft.com/technet/security/Bulletin/ms08-054.mspx>
* SECUNIA: 31726
<http://secunia.com/advisories/31726/>
* FRSIRT: FrSIRT/ADV-2008-2522
<http://www.frsirt.com/english/advisories/2008/2522>
* SECTRACK: 1020831
<http://www.securitytracker.com/alerts/2008/Sep/1020831.html>
* BID: 30550
<http://www.securityfocus.com/bid/30550>

CVE Reference:

CVE-2008-2253 (cve.mitre.org, nvd.nist.gov)

• 18098 GDI+ VML Buffer Overrun Vulnerability (MS08-052/954593) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI+ handles gradient sizes. The vulnerability could allow remote code execution if a user browses to a Web site that contains specially crafted content. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

This test case specifically checks the following components:

- Office 2003
- IE 6
- Windows XP
- Windows 2003
- Windows 2008
- Windows Vista

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-052
<http://www.microsoft.com/technet/security/Bulletin/ms08-052.mspx>
* SECUNIA: 31675
<http://secunia.com/advisories/31675/>
* FRSIRT: FrSIRT/ADV-2008-2520
<http://www.frsirt.com/english/advisories/2008/2520>

* SECTRACK: 1020834

<http://securitytracker.com/alerts/2008/Sep/1020834.html>

* BID: 31018

<http://www.securityfocus.com/bid/31018>

CVE Reference:

CVE-2007-5348 (cve.mitre.org, nvd.nist.gov)

• 18099 GDI+ EMF Memory Corruption Vulnerability (MS08-052/954593) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI+ handles memory allocation. The vulnerability could allow remote code execution if a user opens a specially crafted EMF image file or browses to a Web site that contains specially crafted content. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

This test case specifically checks the following components:

- Office 2003
- IE 6
- Windows XP
- Windows 2003
- Windows 2008
- Windows Vista

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-052

<http://www.microsoft.com/technet/security/Bulletin/ms08-052.msp>

* SECUNIA: 31675

<http://secunia.com/advisories/31675/>

* FRSIRT: FrSIRT/ADV-2008-2520

<http://www.frst.com/english/advisories/2008/2520>

* SECTRACK: 1020835

<http://www.securitytracker.com/alerts/2008/Sep/1020835.html>

* BID: 31019

<http://www.securityfocus.com/bid/31019>

CVE Reference:

CVE-2008-3012 (cve.mitre.org, nvd.nist.gov)

• 18104 GDI+ GIF Parsing Vulnerability (MS08-052/954593) (Remote File Checking)

A remote code execution vulnerability exists in the way that GDI+ parses GIF images. The vulnerability could allow remote code execution if a user opens a specially crafted GIF image file or browses to a Web site that contains specially crafted content. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts.

This test case specifically checks the following components:

- Office 2003
- IE 6
- Windows XP
- Windows 2003
- Windows 2008
- Windows Vista

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-052

<http://www.microsoft.com/technet/security/Bulletin/ms08-052.msp>

* SECUNIA: 31675

<http://secunia.com/advisories/31675/>

* FRSIRT: FrSIRT/ADV-2008-2520

<http://www.frst.com/english/advisories/2008/2520>

* SECTRACK: 1020836

<http://www.securitytracker.com/alerts/2008/Sep/1020836.html>

* BID: 31020

<http://www.securityfocus.com/bid/31020>

CVE Reference:

CVE-2008-3013 (cve.mitre.org, nvd.nist.gov)

• **18121 GDI+ WMF Buffer Overrun Vulnerability (MS08-052/954593) (Remote File Checking)**

A remote code execution vulnerability exists in the way that GDI+ allocates memory for WMF image files. The vulnerability could allow remote code execution if a user opens a specially crafted WMF image file or browses to a Web site that contains specially crafted content. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

This test case specifically checks the following components:

- Office 2003
- IE 6
- Windows XP
- Windows 2003
- Windows 2008
- Windows Vista

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

- * MS: MS08-052
<http://www.microsoft.com/technet/security/Bulletin/ms08-052.mspx>
- * SECUNIA: 31675
<http://secunia.com/advisories/31675/>
- * FRSIRT: FrSIRT/ADV-2008-2520
<http://www.frst.com/english/advisories/2008/2520>
- * SECTRACK: 1020837
<http://securitytracker.com/alerts/2008/Sep/1020837.html>
- * BID: 31021
<http://www.securityfocus.com/bid/31021>

CVE Reference:

CVE-2008-3014 (cve.mitre.org, nvd.nist.gov)

• **18122 GDI+ BMP Integer Overflow Vulnerability (MS08-052/954593) (Remote File Checking)**

A remote code execution vulnerability exists in the way that GDI+ handles integer calculations. The vulnerability could allow remote code execution if a user opens a specially crafted BMP image file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

This test case specifically checks the following components:

- Office 2003
- IE 6
- Windows XP
- Windows 2003
- Windows 2008
- Windows Vista

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

- * MS: MS08-052
<http://www.microsoft.com/technet/security/Bulletin/ms08-052.mspx>
- * SECUNIA: 31675
<http://secunia.com/advisories/31675/>
- * FRSIRT: FrSIRT/ADV-2008-2520
<http://www.frst.com/english/advisories/2008/2520>
- * SECTRACK: 1020838
<http://www.securitytracker.com/alerts/2008/Sep/1020838.html>
- * BID: 31022
<http://www.securityfocus.com/bid/31022>

CVE Reference:

CVE-2008-3015 (cve.mitre.org, nvd.nist.gov)

• **18123 Windows Media Encoder Buffer Overrun Vulnerability (MS08-053/954156) (Remote File Checking)**

A remote code execution vulnerability exists in the WMEX.DLL ActiveX control installed by Windows Media Encoder 9 Series. The vulnerability could allow remote code execution if a user views a specially crafted Web page. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

- * MS: MS08-053
<http://www.microsoft.com/technet/security/Bulletin/ms08-053.msp>
- * SECUNIA: 31724
<http://secunia.com/advisories/31724/>
- * FRSIRT: FrSIRT/ADV-2008-2521
<http://www.frstirt.com/english/advisories/2008/2521>
- * SECTRACK: 1020832
<http://securitytracker.com/alerts/2008/Sep/1020832.html>
- * BID: 31065
<http://www.securityfocus.com/bid/31065>

CVE Reference:

CVE-2008-3008 (cve.mitre.org, nvd.nist.gov)

• **18124 Uniform Resource Locator Validation Error Vulnerability (MS08-055/955047) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles specially crafted URLs using the OneNote protocol handler (onenote://). The vulnerability could allow remote code execution if a user clicks a specially crafted OneNote URL. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

- * MS: MS08-055
<http://www.microsoft.com/technet/security/Bulletin/ms08-055.msp>
- * SECUNIA: 31744
<http://secunia.com/advisories/31744/>
- * FRSIRT: FrSIRT/ADV-2008-2523
<http://www.frstirt.com/english/advisories/2008/2523>
- * SECTRACK: 1020833
<http://securitytracker.com/alerts/2008/Sep/1020833.html>
- * BID: 31067
<http://www.securityfocus.com/bid/31067>

CVE Reference:

CVE-2008-3007 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2007-5348 Microsoft CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in the vector graphics link library in gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via an image file with crafted gradient sizes, aka "GDI+ VML Buffer Overrun Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-052.msp>

CVE Reference: [CVE-2007-5348](#)

• **CVE-2008-2253 Microsoft CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Microsoft Windows Media Player 11 allows remote attackers to execute arbitrary code via a crafted audio-only file that is streamed from a Server-Side Playlist (SSPL) on Windows Media Server, aka "Windows Media Player Sampling Rate Vulnerability." <http://www.microsoft.com/technet/security/Bulletin/MS08-054.msp>
Security updates are available from Microsoft Update, Windows Update, and Office Update. Security updates are also available from the Microsoft Download Center. You can find them most easily by doing a keyword search for "security update." *Windows Server 2008 server core installation not affected. The vulnerability addressed by this update does not affect supported editions of Windows Server 2008 if Windows Server 2008 was installed using the Server Core installation option, even though the files affected by this vulnerability may be present on the system. However, users with the affected files will still be offered this update because the update files are newer (with higher version numbers) than the files that are currently on your system. For more information on this installation option, see Server Core. Note that the Server Core installation option does not apply to certain editions of Windows Server 2008; see Compare Server Core Installation Options.

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-054.msp>

CVE Reference: [CVE-2008-2253](#)

• **CVE-2008-3007 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office XP SP3, 2003 SP2 and SP3, 2007 Office System Gold and SP1, and Office OneNote 2007 Gold and SP1 allow remote attackers to execute arbitrary code via a crafted onenote:// URL, aka "Uniform Resource Locator Validation Error Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-055.msp>

CVE Reference: [CVE-2008-3007](#)

• **CVE-2008-3008 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in a certain ActiveX control in wmex.dll in Microsoft Windows Media Encoder 9 Series allows remote attackers to execute arbitrary code via unspecified vectors, aka "Windows Media Encoder Buffer Overrun Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-053.msp>

CVE Reference: [CVE-2008-3008](#)

• **CVE-2008-3012 Microsoft CVSS 2.0 Score = 9.3**

gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 does not properly perform memory allocation, which allows remote attackers to execute arbitrary code via a malformed EMF image file, aka "GDI+ EMF Memory Corruption Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-052.msp>

CVE Reference: [CVE-2008-3012](#)

• **CVE-2008-3013 Microsoft CVSS 2.0 Score = 9.3**

gdipplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a GIF image file with a "malformed graphic control extension," aka "GDI+ GIF Parsing Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-052.msp>

CVE Reference: [CVE-2008-3013](#)

• **CVE-2008-3014 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in gdipplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a malformed WMF image file that triggers improper memory allocation, aka "GDI+ WMF Buffer Overrun Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-052.msp>

CVE Reference: [CVE-2008-3014](#)

• **CVE-2008-3015 Microsoft CVSS 2.0 Score = 9.3**

Integer overflow in gdipplus.dll in GDI+ in Microsoft Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a BMP image file with a malformed BitMapInfoHeader that triggers a buffer overflow, aka "GDI+ BMP Integer Overflow Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-052.msp>

CVE Reference: [CVE-2008-3015](#)

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. <http://www.infosyssec.org/infosyssec/>

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com

About SecureScout

SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.

SecureScout is a trademark of NexantiS Corporation.

netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:

Customers in America and Northern Europe contact us at info@netVigilance.com

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net