

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

[Winny \(WinNY\) software Scanner](#) - The S4 Winny Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if the peer-to-peer software Winny is installed and running.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winnyscanner>

This Week in Review

Some good advice on data security. Is it really legal to present social security numbers on web? Data breaches continue to sky rocket. Your medical information at risk.

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

• The key to data security: Separation of duties

August 27, 2008 (CSO) Separation of duties is a key concept of internal controls. This objective is achieved by disseminating the tasks and associated privileges for a specific security process among multiple people.

Separation of duties is a common policy when people are handling money so that fraud requires collusion of two or more parties. This greatly reduces the likelihood of crime. Information should be handled in the same way. It is therefore imperative that an organization be designed so that no person acting alone can compromise security controls.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113647&source=rss_topic1

• Judge lets privacy advocate keep Social Security numbers on Web site

August 27, 2008 (Computerworld) Can a state government prohibit an individual from posting Social Security numbers online that were easily and legally obtained from government Web sites?

In a memorandum issued last Friday (download PDF), Judge Robert Payne of the U.S. District Court for the Eastern District of Virginia ruled that it would be unconstitutional for the state of Virginia to force Ostergren to remove from her site Social Security numbers that she legally obtained from public records. A memorandum opinion does not create a legal precedent.

Ostergren, who has been working for several years to force Virginia county governments to redact Social Security numbers and other personal data from records posted online, contended in the suit that the law was passed specifically to curtail her campaign.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113642&source=rss_topic1

• Data breaches already surpass 2007 total

The number of reported data breaches has already surpassed 2007's total, according to a report from Identity Theft Resource Center.

"The breach list, however, doesn't reveal exactly how many records were compromised," Foley said.

"More states and organizations are required to report breaches," he said, "and more consumers want to hear about them."

SC Magazine

Full Story :

<http://www.scmagazineus.com/Data-breaches-already-surpass-2007-total/article/115920/>

• Medical identity thefts on the rise

Medical identity theft is increasing, in part because of the wealth of personal information available in medical records, experts say. And much of this identity theft is coming from within the medical community.

"It's more information than you'll find almost anywhere else, which is why medical identity theft is increasing faster than retail or banking thefts," King said. "Also, in health care, that information is shared with other doctors, insurance companies, other health care facilities, and there's a risk of those other systems not being as secure as they should be."

"That infects the computer the employee is working from, and it can launch attacks on information on the server," he said.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Medical-identity-thefts-on-the-rise/article/115880/>

New Vulnerabilities Tested in SecureScout

• 18049 RealPlayer (10/10.5) ActiveX import method buffer overflow vulnerability (Remote File Checking)

Stack-based buffer overflow in a certain ActiveX control in rjbdll.dll in RealNetworks RealPlayer Enterprise, RealPlayer 10, and RealPlayer 10.5 before build 6.0.12.1675 allows remote attackers to execute arbitrary code by importing a file into a media library and then deleting this file.

The vulnerability is reported in:

RealPlayer 10.5 (6.0.12.1040-6.0.12.1663, 6.0.12.1698, 6.0.12.1741

RealPlayer 10

RealPlayer Enterprise

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

References:

* BUGTRAQ: 20080725 <http://www.zerodayinitiative.com/advisories/ZDI-08-046>
<http://www.securityfocus.com/archive/1/archive/1/494778/100/0/threaded>

* MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-046/>
* CONFIRM:
http://service.real.com/realplayer/security/07252008_player/en/
* CERT-VN: VU#461187
<http://www.kb.cert.org/vuls/id/461187>
* BID: 30376
<http://www.securityfocus.com/bid/30376>
* SECTRAK: 1020565
<http://securitytracker.com/id?1020565>
* XF: realplayer-rjbdll-active-x-bo(44013)
<http://xforce.iss.net/xforce/xfdb/44013>

CVE Reference:

CVE-2008-3066 (cve.mitre.org, nvd.nist.gov)

• 18070 IPsec Policy Information Disclosure Vulnerability (MS08-047/953733) (Remote File Checking)

An information disclosure vulnerability exists in the manner in which IPsec policies are imported to Windows Server 2008 domains from Windows Server 2003 domains. This vulnerability could cause systems to ignore IPsec policies and transmit network traffic in clear text. This, in turn, would potentially disclose information intended to be encrypted on the network. An attacker intercepting the traffic on the network would be able to view and possibly modify the contents of the traffic. Note that this vulnerability would not allow an attacker to execute code or to elevate their user rights directly. It could be used to collect useful information to try to further compromise the affected system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Medium**

References:

* MS: MS08-047
<http://www.microsoft.com/technet/security/bulletin/ms08-047.msp>
* BID: 30634
<http://www.securityfocus.com/bid/30634>
* FRSIRT: ADV-2008-2351
<http://www.frsirt.com/english/advisories/2008/2351>
* SECTRAK: 1020678
<http://www.securitytracker.com/id?1020678>
* SECUNIA: 31411
<http://secunia.com/advisories/31411>

CVE Reference:

CVE-2008-2246 (cve.mitre.org, nvd.nist.gov)

• 18071 Event System Vulnerability (CVE-2008-1457) (MS08-049/950974) (Remote File Checking)

A remote code execution vulnerability exists because the Microsoft Windows Event System does not correctly validate user subscriptions requests when created. The vulnerability could allow remote code execution. 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 administrative rights.

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

References:

* MS: MS08-049
<http://www.microsoft.com/technet/security/Bulletin/MS08-049.msp>
* BID: 30584
<http://www.securityfocus.com/bid/30584>
* FRSIRT: ADV-2008-2353
<http://www.frsirt.com/english/advisories/2008/2353>
* SECUNIA: 31417
<http://secunia.com/advisories/31417>

CVE Reference:

CVE-2008-1457 (cve.mitre.org, nvd.nist.gov)

• 18072 Event System Vulnerability (CVE-2008-1456) (MS08-049/950974) (Remote File Checking)

A remote code execution vulnerability exists because the Microsoft Windows Event System does not correctly validate the range of indexes when calling an array of function pointers. The vulnerability could allow remote code execution. 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 administrative rights.

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

References:

- * MS: MS08-049
<http://www.microsoft.com/technet/security/Bulletin/MS08-049.msp>
- * FRSIRT: ADV-2008-2353
<http://www.frsirt.com/english/advisories/2008/2353>
- * SECUNIA: 31417
<http://secunia.com/advisories/31417>

CVE Reference:

CVE-2008-1456 (cve.mitre.org, nvd.nist.gov)

• 18073 URL Parsing Cross-Domain Information Disclosure Vulnerability (MS08-048/951066) (Remote File Checking)

An information disclosure vulnerability exists in Outlook Express and Windows Mail because the MHTML protocol handler incorrectly interprets MHTML URL redirections that could potentially bypass Internet Explorer domain restrictions when returning MHTML content. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If the user viewed the Web page through Internet Explorer, the vulnerability could potentially allow information disclosure. An attacker who successfully exploited this vulnerability could read data from another Internet Explorer domain or the local computer.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Medium**

References:

- * MS: MS08-048
<http://www.microsoft.com/technet/security/bulletin/ms08-048.msp>
- * BID: 30585
<http://www.securityfocus.com/bid/30585>
- * FRSIRT: ADV-2008-2352
<http://www.frsirt.com/english/advisories/2008/2352>
- * SECTrack: 1020679
<http://www.securitytracker.com/id?1020679>
- * SECTrack: 1020680
<http://www.securitytracker.com/id?1020680>
- * SECUNIA: 31415
<http://secunia.com/advisories/31415>

CVE Reference:

CVE-2008-1448 (cve.mitre.org, nvd.nist.gov)

• 18074 Messenger Information Disclosure Vulnerability (MS08-050/955702) (Remote File Checking)

An information disclosure vulnerability exists in supported versions of Windows Messenger. Scripting of a particular ActiveX control, Messenger.UIAutomation.1, could allow information disclosure from these programs in the context of the logged-on user. An attacker could change state, get contact information, and initiate audio and video chat sessions without the knowledge of the logged-on user. An attacker could also capture the user's logon ID and remotely log on to the user's Messenger client as that user.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Medium**

References:

- * MS: MS08-050
<http://www.microsoft.com/technet/security/bulletin/ms08-050.msp>
- * BID: 30551
<http://www.securityfocus.com/bid/30551>
- * FRSIRT: ADV-2008-2354
<http://www.frsirt.com/english/advisories/2008/2354>
- * SECTrack: 1020681
<http://www.securitytracker.com/id?1020681>
- * SECUNIA: 31446
<http://secunia.com/advisories/31446>

CVE Reference:

CVE-2008-0082 (cve.mitre.org, nvd.nist.gov)

• 18075 Word Record Parsing Vulnerability (MS08-042/955048) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Word handles specially crafted Word files. The vulnerability could allow remote code execution if a user opens a specially crafted Word file that includes a malformed record value. 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: **Gather Info** Risk: **High**

References:

* MISC:

<http://isc.sans.org/diary.html?storyid=4696>

* CONFIRM:

<http://blogs.technet.com/msrc/archive/2008/07/08/vulnerability-in-microsoft-word-could-allow-remote-code-execution.aspx>

* CONFIRM:

<http://www.microsoft.com/technet/security/advisory/953635.msp>

* BID: 30124

<http://www.securityfocus.com/bid/30124>

* FRSIRT: ADV-2008-2028

<http://www.frsirt.com/english/advisories/2008/2028>

* SECUNIA: 30975

<http://secunia.com/advisories/30975>

* XF: microsoft-word-unspecified-code-execution(43663)

<http://xforce.iss.net/xforce/xfdb/43663>

* MS: MS08-042

<http://www.microsoft.com/technet/security/bulletin/ms08-042.msp>

CVE Reference:

CVE-2008-2244 (cve.mitre.org, nvd.nist.gov)

• 18076 Winamp "NowPlaying" Unspecified Vulnerability (Remote File Checking)

Unspecified vulnerability in the NowPlaying functionality in NullSoft Winamp before 5.541 has unknown impact and attack vectors.

The vulnerability is confirmed in version prior to 5.541.

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

References:

* CONFIRM:

<http://forums.winamp.com/showthread.php?threadid=295505>

* BID: 30539

<http://www.securityfocus.com/bid/30539>

* SECUNIA: 31371

<http://secunia.com/advisories/31371>

CVE Reference:

CVE-2008-3567 (cve.mitre.org, nvd.nist.gov)

• 18077 Winamp libmp4v2.dll MP4 file arbitrary code execution Vulnerability (Remote File Checking)

libmp4v2.dll in Winamp 5.02 through 5.34 allows user-assisted remote attackers to execute arbitrary code via a certain .MP4 file. NOTE: some of these details are obtained from third party information.

The vulnerability is confirmed in version between 5.02 and 5.34.

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

References:

* MILWORM: 3823

<http://www.milw0rm.com/exploits/3823>

* BID: 23723

<http://www.securityfocus.com/bid/23723>

* FRSIRT: ADV-2007-1594

<http://www.frsirt.com/english/advisories/2007/1594>

* SECTRAK: 1017993

<http://securitytracker.com/id?1017993>

* SECUNIA: 25089
<http://secunia.com/advisories/25089>
* XF: winamp-mp4-code-execution(34030)
<http://xforce.iss.net/xforce/xfdb/34030>

CVE Reference:

CVE-2007-2498 (cve.mitre.org, nvd.nist.gov)

• 18078 Winamp crafted unicode in a .mp4 file, arbitrary code execution Vulnerability (Remote File Checking)

Stack-based buffer overflow in Nullsoft Winamp 5.32 allows user-assisted remote attackers to execute arbitrary code via crafted unicode in a .mp4 file, with crafted tags, contained in a certain .rar archive. NOTE: for exploitation, the victim must select a certain menu option at the time of the attack.

The vulnerability is confirmed in version 5.x before 5.5.

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

References:

* BUGTRAQ: 20071208 Nullsoft Winamp MP4 tags Stack Overflow
<http://www.securityfocus.com/archive/1/archive/1/484776/100/0/threaded>
* SREASON: 3456
<http://securityreason.com/securityalert/3456>

CVE Reference:

CVE-2007-6403 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-4110 Microsoft CVSS 2.0 Score = 10.0

Buffer overflow in the SQLVDIRLib.SQLVDirControl ActiveX control in Tools\Binn\sqlvdir.dll in Microsoft SQL Server 2000 (aka SQL Server 8.0) allows remote attackers to cause a denial of service (browser crash) or possibly execute arbitrary code via a long URL in the second argument to the Connect method. NOTE: this issue might only be exploitable in limited browser configurations.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/45186>
BID: <http://www.securityfocus.com/bid/31129>
BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496232/100/0/threaded>

CVE Reference: [CVE-2008-4110](#)

• CVE-2008-4301 Microsoft CVSS 2.0 Score = 10.0

** DISPUTED ** A certain ActiveX control in iisext.dll in Microsoft Internet Information Services (IIS) allows remote attackers to set a password via a string argument to the SetPassword method. NOTE: this issue could not be reproduced by a reliable third party. In addition, the original researcher is unreliable. Therefore the original disclosure is probably erroneous.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/45587>
BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/496694/100/0/threaded>
VIM: <http://www.attribution.org/pipermail/vim/2008-October/002081.html>

CVE Reference: [CVE-2008-4301](#)

• 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](#)

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