

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

[Task Scheduler Vulnerability Scanner](#) - The S4 Task Scheduler Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Task Scheduler flaw (MS04-022).

Download Here:

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

This Week in Review

PCI updates requirements. FTP plans workshop around RFID. Data encryption becoming law.

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

• Changes to PCI standard not expected to up ante on protecting payment card data

August 20, 2008 (Computerworld) The group that administers the Payment Card Industry Data Security Standard — or PCI, for short — this week released a summary of the changes that are being made to the requirements in a revision scheduled to be published in October.

The PCI standard was created by the major credit card companies, including Visa, MasterCard and American Express, to try to prevent the theft of credit and debit card data from retail systems. The standard, which went into effect in June 2005, outlines 12 broad security controls that retailers, online merchants, data processors and other businesses must implement to protect cardholder data. Companies that fail to meet the requirements are subject to fines and potentially can be barred from processing payment card transactions.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113104&source=rss_topic1

• **FTC to study RFID as use becomes more widespread**

The Federal Trade Commission on Wednesday announced plans to host a workshop next month that will study how the growing use of radio frequency identification technology (RFID) may impact consumer security and privacy.

Expected to attend the free workshop are industry representatives, government officials and consumer advocates from the United States and Europe.

Participants will discuss the increased use of RFID technology in credit card purchases and transit systems and by retailers to tag merchandise.

SC Magazine

Full Story :

<http://www.scmagazineus.com/FTC-to-study-RFID-as-use-becomes-more-widespread/article/115721/>

• **New laws require data encryption**

The state of Iowa has passed a data breach law that requires companies to encrypt customer details.

According to Jerome Wendt, president and lead analyst at computer consultancy DCIG Inc., some states do not consider encryption alone to provide sufficient security. For example, Pennsylvania has added a stipulation that companies must have proper encryption key management policies in place. This will guarantee that encrypted data on tape cannot be decrypted should someone manage to get their hands on both the tape and the key used to encrypt it.

He says that it is unclear whether providing a one-word password to the software to encrypt the data is a proper key management policy.

SC Magazine

Full Story :

<http://www.scmagazineus.com/New-laws-require-data-encryption/article/115552/>

• **Internet-threat portal on tap from TippingPoint**

August 19, 2008 (Network World) TippingPoint is beta-testing a Web portal that lets customers view Internet-threat intelligence the company has gathered from around the globe, as well as polls of how other customers are dealing with those threats.

Other vendors, including McAfee and Symantec, also have portals detailing threats of the type their products can combat.

The portal presents the kinds of attacks that are occurring and the IP addresses where they originate. Alongside each threat, the portal lists the number of which TippingPoint filter or filters will deal with the problem. It also tells whether that filter is turned on as a default on TippingPoint's IPS so customers can figure out more easily whether they need to make a change.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112958&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• **18050 Microsoft Color Management System Vulnerability (MS08-046/952954) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Color Management System (MSCMS) module of the Microsoft ICM component handles memory allocation. The vulnerability could allow remote code execution if a user opens a specially crafted 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.

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

References:

* MS: MS08-046

<http://www.microsoft.com/technet/security/bulletin/ms08-046.msp>

* CERT-VN: VU#309739

<http://www.kb.cert.org/vuls/id/309739>

* BID: 30594

<http://www.securityfocus.com/bid/30594>

* FRSIRT: ADV-2008-2350

<http://www.frsirt.com/english/advisories/2008/2350>

* SECTRACK: 1020675

<http://www.securitytracker.com/id?1020675>

* SECUNIA: 31385

<http://secunia.com/advisories/31385>

CVE Reference:

CVE-2008-2245 (cve.mitre.org, nvd.nist.gov)

• 18057 Snapshot Viewer Arbitrary File Download Vulnerability (MS08-041/955617) (Remote File Checking)

A remote code execution vulnerability exists in the ActiveX control for the Snapshot Viewer for Microsoft Access. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

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

References:

* CONFIRM:

<http://www.microsoft.com/technet/security/advisory/955179.msp>

* CERT: TA08-189A

<http://www.us-cert.gov/cas/techalerts/TA08-189A.html>

* CERT-VN: VU#837785

<http://www.kb.cert.org/vuls/id/837785>

* BID: 30114

<http://www.securityfocus.com/bid/30114>

* FRSIRT: ADV-2008-2012

<http://www.frsirt.com/english/advisories/2008/2012/references>

* SECTRACK: 1020433

<http://www.securitytracker.com/id?1020433>

* SECUNIA: 30883

<http://secunia.com/advisories/30883>

* XF: microsoft-snapshotviewer-code-execution(43613)

<http://xforce.iss.net/xforce/xfdb/43613>

* MS: MS08-041

<http://www.microsoft.com/technet/security/bulletin/ms08-041.msp>

CVE Reference:

CVE-2008-2463 (cve.mitre.org, nvd.nist.gov)

• 18062 PowerPoint Memory Allocation Vulnerability (MS08-051/949785) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint Viewer 2003 handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

* MS: MS08-051

<http://www.microsoft.com/technet/security/bulletin/ms08-051.msp>

* FRSIRT: ADV-2008-2355

<http://www.frsirt.com/english/advisories/2008/2355>

* SECUNIA: 31453

<http://secunia.com/advisories/31453>

CVE Reference:

CVE-2008-0120 (cve.mitre.org, nvd.nist.gov)

• 18063 PowerPoint Memory Calculation Vulnerability (MS08-051/949785) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint Viewer 2003 handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

- * MS: MS08-051
<http://www.microsoft.com/technet/security/bulletin/ms08-051.msp>
- * FRSIRT: ADV-2008-2355
<http://www.frsirt.com/english/advisories/2008/2355>
- * SECUNIA: 31453
<http://secunia.com/advisories/31453>

CVE Reference:

CVE-2008-0121 (cve.mitre.org, nvd.nist.gov)

• 18064 PowerPoint Parsing Overflow Vulnerability (MS08-051/949785) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

- * MS: MS08-051
<http://www.microsoft.com/technet/security/bulletin/ms08-051.msp>
- * FRSIRT: ADV-2008-2355
<http://www.frsirt.com/english/advisories/2008/2355>
- * SECUNIA: 31453
<http://secunia.com/advisories/31453>

CVE Reference:

CVE-2008-1455 (cve.mitre.org, nvd.nist.gov)

• 18065 Microsoft Malformed EPS Filter Vulnerability (MS08-044/924090) (Remote File Checking)

A remote code execution vulnerability exists in the way that a Microsoft Office filter handles a malformed graphics image. An attacker could exploit the vulnerability by constructing a specially crafted Encapsulated PostScript (EPS) file that could allow remote code execution if a user opened the file with a Microsoft Office application. Such a specially crafted file might be included as an e-mail attachment, or hosted on a malicious or compromised Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

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

References:

- * MS: MS08-044
<http://www.microsoft.com/technet/security/Bulletin/MS08-044.msp>
- * BID: 30595
<http://www.securityfocus.com/bid/30595>
- * FRSIRT: ADV-2008-2348
<http://www.frsirt.com/english/advisories/2008/2348>
- * SECTRACK: 1020673
<http://www.securitytracker.com/id?1020673>
- * SECUNIA: 31336

<http://secunia.com/advisories/31336>

CVE Reference:

CVE-2008-3019 (cve.mitre.org, nvd.nist.gov)

• **18066 Microsoft Malformed PICT Filter Vulnerability (MS08-044/924090) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles a PICT-format image file. The vulnerability could be exploited when a Microsoft Office application opens a specially crafted PICT-format image file. Such a specially crafted file might be included as an e-mail attachment, or hosted on a malicious or compromised Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

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

References:

* MS: MS08-044

<http://www.microsoft.com/technet/security/Bulletin/MS08-044.msp>

* BID: 30597

<http://www.securityfocus.com/bid/30597>

* FRSIRT: ADV-2008-2348

<http://www.frsirt.com/english/advisories/2008/2348>

* SECTRACK: 1020673

<http://www.securitytracker.com/id?1020673>

* SECUNIA: 31336

<http://secunia.com/advisories/31336>

CVE Reference:

CVE-2008-3018 (cve.mitre.org, nvd.nist.gov)

• **18067 Microsoft PICT Filter Parsing Vulnerability (MS08-044/924090) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles a PICT-format image file. The vulnerability could be exploited when either a Microsoft Office application opens a specially crafted PICT-format image file. Such a specially crafted file might be included as an e-mail attachment, or hosted on a malicious or compromised Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

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

References:

* MS: MS08-044

<http://www.microsoft.com/technet/security/Bulletin/MS08-044.msp>

* BID: 30598

<http://www.securityfocus.com/bid/30598>

* FRSIRT: ADV-2008-2348

<http://www.frsirt.com/english/advisories/2008/2348>

* SECTRACK: 1020673

<http://www.securitytracker.com/id?1020673>

* SECUNIA: 31336

<http://secunia.com/advisories/31336>

CVE Reference:

CVE-2008-3021 (cve.mitre.org, nvd.nist.gov)

• **18068 Microsoft Malformed BMP Filter Vulnerability (MS08-044/924090) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles a BMP format image file. The vulnerability could be exploited when a Microsoft Office application opens a specially crafted BMP-format image file. Such a specially crafted file might be included as an e-mail attachment, or hosted on a malicious or compromised Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

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

References:

* MS: MS08-044

<http://www.microsoft.com/technet/security/Bulletin/MS08-044.msp>

* BID: 30599

<http://www.securityfocus.com/bid/30599>

* FRSIRT: ADV-2008-2348

<http://www.frsirt.com/english/advisories/2008/2348>

* SECTRACK: 1020673

<http://www.securitytracker.com/id?1020673>

* SECUNIA: 31336

<http://secunia.com/advisories/31336>

CVE Reference:

CVE-2008-3020 (cve.mitre.org, nvd.nist.gov)

• 18069 Microsoft Office WPG Image File Heap Corruption Vulnerability (MS08-044/924090) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office handles a WordPerfect Graphics (WPG) format image file. The vulnerability could be exploited when Microsoft Office opens a specially crafted WPG-format image file or a WordPerfect document file with a malformed WPG image embedded. Such a specially crafted file might be included as an e-mail attachment, or hosted on a malicious or compromised Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

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

References:

* MS: MS08-044

<http://www.microsoft.com/technet/security/Bulletin/MS08-044.mspx>

* BID: 30600

<http://www.securityfocus.com/bid/30600>

* FRSIRT: ADV-2008-2348

<http://www.frsirt.com/english/advisories/2008/2348>

* SECTRACK: 1020673

<http://www.securitytracker.com/id?1020673>

* SECUNIA: 31336

<http://secunia.com/advisories/31336>

CVE Reference:

CVE-2008-3460 (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](http://cve.mitre.org/cve/2008/4110)

• CVE-2008-3704 Microsoft CVSS 2.0 Score = 9.3

Stack-based buffer overflow in the MaskedEdit ActiveX control in Msmask32.ocx 6.0.81.69, and possibly other versions before 6.0.84.18, in Microsoft Visual Studio 6.0 allows remote attackers to execute arbitrary code via a long Mask parameter, as exploited in the wild in August 2008. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.

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

References:

BID: <http://www.securityfocus.com/bid/30674>

CVE Reference: [CVE-2008-3704](#)

• **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