

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

[Spida Digispid Worm Scanner](#) - The S4 Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

Download Here:

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

This Week in Review

When and where to disclose security flaws. U.S. legal system falling behind. web providers tracking users. Generation divide in security.

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

• Cybercriminal prosecutions falling way behind

The U.S. legal system is failing to bring prosecutions in cybercrime cases. This is despite being presented with online fraud and abuse complaints that number in the thousands.

The report's authors claim that most states supplied a top 10 list that ranked general consumer complaint categories. In 2007, 24 out of the 30 states that did reported an internet-related category within their top 10.

The researchers claim authorities must do more.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Cybercriminal-prosecutions-falling-way-behind/article/115437/>

• Web providers admit to tracking users without their knowledge

Several internet network operators admitted to a Congressional subcommittee that they use targeted-advertising technology without explicitly informing customers, according to the U.S. House Energy and Commerce Committee.

While more than a dozen companies responded to the inquiry by stating they do not target advertising based on individual customer habits, most of them have either run targeted-advertising trials or actively engage in some behavioral advertising.

Jessica Schafer, communications director for committee member Rep. Edward Markey (D-Mass.), told SCMagazineUS.com on Wednesday that staff members are still analyzing the responses from companies. However, Markey is emphatic that online users have a right to explicitly know when their broadband provider is tracking their activity and collecting potentially sensitive and personal information.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Web-providers-admit-to-tracking-users-without-their-knowledge/article/115332/>

• Security and the generational divide

August 8, 2008 (CSO) The generation gap. It's a term that has been used for decades to describe the differences between people in various age groups. Corporations are constantly considering what makes different generations tick when it comes to recruiting and retaining employees. But security experts say companies also need to examine age-based perspectives and habits when it comes to risk assessment and policies.

Gen Y employees, workers born after 1980, are-tech savvy and have a short attention span Baby Boomers, born between 1946 and 1965, are loyal and dependable, the original workaholics Gen Xers, once known as the slacker generation born between 1965 and 1980, tend to be cynical and independent

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112100&source=rss_topic1

• Legal flap over Defcon talk exposes divide on disclosing security flaws

August 15, 2008 (Computerworld) A court order put a stop to a planned presentation at the Defcon hackers convention by three MIT students who found security flaws in the electronic ticketing system used by the mass transit authority in Boston. But the ruling reopened the schism in the IT security community over the issue of how vulnerabilities should be publicly disclosed.

Others, though, see the case involving the students and the Massachusetts Bay Transportation Authority (MBTA) as another example of publicity-hungry security researchers driven more by ego and the desire for fame than by any sincere interest in improving security.

In an affidavit, the MBTA claimed that the students didn't give it sufficient information about the vulnerabilities beforehand. The transit authority added that it wasn't trying to permanently gag the students, but that it wanted some time to determine the validity and seriousness of the flaws and a course of action for addressing them.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112698&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 18051 HTML Objects Memory Corruption Vulnerability (CVE-2008-2254) (MS08-045/953838) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer due to attempts to access uninitialized memory in certain situations. 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:

* HP: HPSBST02360

<http://marc.info/?l=bugtraq&m=121915960406986&w=2>

* MS: MS08-045

<http://www.microsoft.com/technet/security/bulletin/ms08-045.mspx>

* BID: 30614

<http://www.securityfocus.com/bid/30614>

* FRSIRT: ADV-2008-2349

<http://www.frsirt.com/english/advisories/2008/2349>

* SECTRACK: 1020674

<http://www.securitytracker.com/id?1020674>

* SECUNIA: 31375

<http://secunia.com/advisories/31375>

CVE Reference:

CVE-2008-2254 (cve.mitre.org, nvd.nist.gov)

• 18052 HTML Objects Memory Corruption Vulnerability (CVE-2008-2255) (MS08-045/953838) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer due to attempts to access uninitialized memory in certain situations. 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:

* HP: HPSBST02360

<http://marc.info/?l=bugtraq&m=121915960406986&w=2>

* MS: MS08-045

<http://www.microsoft.com/technet/security/bulletin/ms08-045.mspx>

* FRSIRT: ADV-2008-2349

<http://www.frsirt.com/english/advisories/2008/2349>

* SECTRACK: 1020674

<http://www.securitytracker.com/id?1020674>

* SECUNIA: 31375

<http://secunia.com/advisories/31375>

CVE Reference:

CVE-2008-2255 (cve.mitre.org, nvd.nist.gov)

• 18053 Uninitialized Memory Corruption Vulnerability (MS08-045/953838) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or that has been deleted. 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:

* HP: HPSBST02360

<http://marc.info/?l=bugtraq&m=121915960406986&w=2>

* MS: MS08-045

<http://www.microsoft.com/technet/security/bulletin/ms08-045.mspx>

* BID: 30611

<http://www.securityfocus.com/bid/30611>

* FRSIRT: ADV-2008-2349

<http://www.frsirt.com/english/advisories/2008/2349>

* SECTRACK: 1020674

<http://www.securitytracker.com/id?1020674>

* SECUNIA: 31375

<http://secunia.com/advisories/31375>

CVE Reference:

CVE-2008-2256 (cve.mitre.org, nvd.nist.gov)

• 18054 HTML Objects Memory Corruption Vulnerability (CVE-2008-2257) (MS08-045/953838) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer due to attempts to access uninitialized memory in certain situations. 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:

- * BUGTRAQ: 20080812 ZDI-08-050: Microsoft Internet Explorer XHTML Rendering Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/495430/100/0/threaded>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-050/>
- * HP: HPSBST02360
<http://marc.info/?l=bugtraq&m=121915960406986&w=2>
- * MS: MS08-045
<http://www.microsoft.com/technet/security/bulletin/ms08-045.msp>
- * BID: 30613
<http://www.securityfocus.com/bid/30613>
- * FRSIRT: ADV-2008-2349
<http://www.frsirt.com/english/advisories/2008/2349>
- * SECTRACK: 1020674
<http://www.securitytracker.com/id?1020674>
- * SECUNIA: 31375
<http://secunia.com/advisories/31375>

CVE Reference:

CVE-2008-2257 (cve.mitre.org, nvd.nist.gov)

• 18055 HTML Objects Memory Corruption Vulnerability (CVE-2008-2258) (MS08-045/953838) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer due to attempts to access uninitialized memory in certain situations. 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:

- * BUGTRAQ: 20080812 ZDI-08-051: Microsoft Internet Explorer Table Layout Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/495431/100/0/threaded>
- * MISC:
<http://www.zerodayinitiative.com/advisories/ZDI-08-051/>
- * HP: HPSBST02360
<http://marc.info/?l=bugtraq&m=121915960406986&w=2>
- * MS: MS08-045
<http://www.microsoft.com/technet/security/bulletin/ms08-045.msp>
- * BID: 30610
<http://www.securityfocus.com/bid/30610>
- * FRSIRT: ADV-2008-2349
<http://www.frsirt.com/english/advisories/2008/2349>
- * SECTRACK: 1020674
<http://www.securitytracker.com/id?1020674>
- * SECUNIA: 31375
<http://secunia.com/advisories/31375>

CVE Reference:

CVE-2008-2258 (cve.mitre.org, nvd.nist.gov)

• 18056 HTML Component Handling Vulnerability (MS08-045/953838) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer handles argument validation in print preview handling. 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 rights as the logged on user.

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

References:

- * HP: HPSBST02360
<http://marc.info/?l=bugtraq&m=121915960406986&w=2>

* MS: MS08-045
<http://www.microsoft.com/technet/security/bulletin/ms08-045.mspx>
* BID: 30612
<http://www.securityfocus.com/bid/30612>
* FRSIRT: ADV-2008-2349
<http://www.frsirt.com/english/advisories/2008/2349>
* SECTRACK: 1020674
<http://www.securitytracker.com/id?1020674>
* SECUNIA: 31375
<http://secunia.com/advisories/31375>

CVE Reference:

CVE-2008-2259 (cve.mitre.org, nvd.nist.gov)

• **18058 Excel Indexing Validation Vulnerability (MS08-043/954066) (Remote File Checking)**

A remote code execution vulnerability exists in the way Excel processes index values when loading Excel files into memory. An attacker could exploit the vulnerability by opening a specially crafted file which could be hosted on a Web site, or included as an e-mail attachment.

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

References:

* IDEFENSE: 20080812 Microsoft Excel Chart AxesSet Invalid Array Index Vulnerability
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=740>
* HP: HPSBST02360
<http://marc.info/?l=bugtraq&m=121915960406986&w=2>
* MS: MS08-043
<http://www.microsoft.com/technet/security/Bulletin/MS08-043.mspx>
* BID: 30638
<http://www.securityfocus.com/bid/30638>
* FRSIRT: ADV-2008-2347
<http://www.frsirt.com/english/advisories/2008/2347>
* SECTRACK: 1020670
<http://www.securitytracker.com/id?1020670>
* SECUNIA: 31454
<http://secunia.com/advisories/31454>

CVE Reference:

CVE-2008-3004 (cve.mitre.org, nvd.nist.gov)

• **18059 Excel Index Array Vulnerability (MS08-043/954066) (Remote File Checking)**

A remote code execution vulnerability exists in the way Excel processes an array index when loading Excel files into memory. An attacker could exploit the vulnerability by opening a specially crafted file which could be hosted on a Web site, or included as an e-mail attachment.

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

References:

* IDEFENSE: 20080812 Microsoft Excel FORMAT Record Invalid Array Index Vulnerability
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=741>
* HP: HPSBST02360
<http://marc.info/?l=bugtraq&m=121915960406986&w=2>
* MS: MS08-043
<http://www.microsoft.com/technet/security/Bulletin/MS08-043.mspx>
* BID: 30639
<http://www.securityfocus.com/bid/30639>
* FRSIRT: ADV-2008-2347
<http://www.frsirt.com/english/advisories/2008/2347>
* SECTRACK: 1020671
<http://www.securitytracker.com/id?1020671>
* SECUNIA: 31454
<http://secunia.com/advisories/31454>

CVE Reference:

CVE-2008-3005 (cve.mitre.org, nvd.nist.gov)

• **18060 Excel Record Parsing Vulnerability (MS08-043/954066) (Remote File Checking)**

A vulnerability exists in the way Excel parses record values when loading Excel files into memory. Depending on the attack scenario, the vulnerability could lead to remote code execution on a user's local Excel client, or it could lead to elevation of privilege within a SharePoint Server.

In an attack against a user's local Excel client, an attacker could exploit the vulnerability by convincing a user to open a specially crafted file which could be hosted on a Web site, or included as an e-mail attachment.

In an attack against a SharePoint site, an attacker would first need an account on the SharePoint site with sufficient rights to upload a specially crafted Excel file and then create a web part using the file on the SharePoint site.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

- * BUGTRAQ: 20080812 ZDI-08-048: Microsoft Excel COUNTRY Record Memory Corruption Vulnerability
<http://www.securityfocus.com/archive/1/archive/1/495428/100/0/threaded>
- * HP: HPSBST02360
<http://marc.info/?l=bugtraq&m=121915960406986&w=2>
- * MS: MS08-043
<http://www.microsoft.com/technet/security/Bulletin/MS08-043.msp>
- * BID: 30640
<http://www.securityfocus.com/bid/30640>
- * FRSIRT: ADV-2008-2347
<http://www.frsirt.com/english/advisories/2008/2347>
- * SECTRACK: 1020672
<http://www.securitytracker.com/id?1020672>
- * SECUNIA: 31454
<http://secunia.com/advisories/31454>
- * SECUNIA: 31455
<http://secunia.com/advisories/31455>

CVE Reference:

CVE-2008-3006 (cve.mitre.org, nvd.nist.gov)

• 18061 Excel Credential Caching Vulnerability (MS08-043/954066) (Remote File Checking)

An elevation of privilege vulnerability exists in Excel 2007 when data connections are made to a remote data sources. An attacker could exploit the vulnerability to gain access to a secured remote data source by opening an .xlsx file that had been explicitly configured not to store credentials to the remote data source.

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

References:

- * HP: HPSBST02360
<http://marc.info/?l=bugtraq&m=121915960406986&w=2>
- * MS: MS08-043
<http://www.microsoft.com/technet/security/Bulletin/MS08-043.msp>
- * BID: 30641
<http://www.securityfocus.com/bid/30641>
- * FRSIRT: ADV-2008-2347
<http://www.frsirt.com/english/advisories/2008/2347>
- * SECTRACK: 1020669
<http://www.securitytracker.com/id?1020669>
- * SECUNIA: 31454
<http://secunia.com/advisories/31454>

CVE Reference:

CVE-2008-3003 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-0082 Microsoft CVSS 2.0 Score = 10.0

An ActiveX control (Messenger.UIAutomation.1) in Windows Messenger 4.7 and 5.1 is marked as safe-for-scripting, which allows remote attackers to "change state," obtain contact information, and establish audio or video connections without notification via unknown vectors.

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

References:

MS: <http://www.microsoft.com/technet/security/bulletin/ms08-050.msp>

BID: <http://www.securityfocus.com/bid/30551>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2354>

SECTRAK: <http://www.securitytracker.com/id?1020681>

SECUNIA: <http://secunia.com/advisories/31446>

CVE Reference: [CVE-2008-0082](#)

• CVE-2008-0120 Microsoft CVSS 2.0 Score = 9.3

A "memory allocation error" in Microsoft PowerPoint Viewer 2003 allows remote attackers to execute arbitrary code via a PowerPoint file with a malformed picture index that triggers memory corruption, aka "Memory Allocation Vulnerability."

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

References:

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

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

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

CVE Reference: [CVE-2008-0120](#)

• CVE-2008-3004 Microsoft CVSS 2.0 Score = 9.3

Microsoft Office Excel 2000 SP3, 2002 SP3, and 2003 SP2 and SP3; Office Excel Viewer 2003; and Office 2004 and 2008 for Mac do not properly validate index values when loading Excel files, which allows remote attackers to execute arbitrary code via a crafted Excel file, aka the "Excel Indexing Validation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-043.msp>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2347>

CVE Reference: [CVE-2008-3004](#)

• CVE-2008-3005 Microsoft CVSS 2.0 Score = 9.3

Microsoft Office Excel 2000 SP3 and 2002 SP3, and Office 2004 and 2008 for Mac, do not properly validate an unspecified array index when loading Excel files, which allows remote attackers to execute arbitrary code via a crafted Excel file, aka the "Excel Index Array Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-043.msp>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2347>

CVE Reference: [CVE-2008-3005](#)

• CVE-2008-3006 Microsoft CVSS 2.0 Score = 9.3

Microsoft Office Excel 2000 SP3, 2002 SP3, 2003 SP2 and SP3, and 2007 Gold and SP1; Office Excel Viewer 2003 Gold and SP3; Office Excel Viewer; Office Compatibility Pack 2007 Gold and SP1; Office SharePoint Server 2007 Gold and SP1; and Office 2004 and 2008 for Mac do not properly parse record values when loading Excel files, which allows remote attackers to execute arbitrary code via a crafted Excel file, aka the "Excel Record Parsing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS08-043.msp>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2347>

CVE Reference: [CVE-2008-3006](#)

• **CVE-2008-3018 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office 2000 SP3, XP SP3, and 2003 SP2; Office Converter Pack; and Works 8 do not properly parse the length of a PICT file, which allows remote attackers to execute arbitrary code via a crafted PICT file, aka the "Malformed PICT Filter Vulnerability," a different vulnerability than CVE-2008-3021.

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

References:

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

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

CVE Reference: [CVE-2008-3018](#)

• **CVE-2008-3019 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office 2000 SP3, XP SP3, and 2003 SP2; Office Converter Pack; and Works 8 do not properly parse the length of an Encapsulated PostScript (EPS) file, which allows remote attackers to execute arbitrary code via a crafted EPS file, aka the "Malformed EPS Filter Vulnerability."

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

References:

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

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

CVE Reference: [CVE-2008-3019](#)

• **CVE-2008-3020 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office 2000 SP3 and XP SP3; Office Converter Pack; and Works 8 do not properly parse the length of a BMP file, which allows remote attackers to execute arbitrary code via a crafted BMP file, aka the "Malformed BMP Filter Vulnerability."

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

References:

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

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

CVE Reference: [CVE-2008-3020](#)

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