

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

Security vendors: Come together. Privacy versus security - a balance. As protection gets better, hackers get better too. Call for new consumer 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

• RSA chief calls for 'inventive collaboration' among security vendors

April 21, 2009 (Computerworld) SAN FRANCISCO -- Two years after suggesting that independent security vendors were headed for extinction, Art Coviello, president of RSA, is calling for "inventive collaboration" among vendors for dealing with the expanding range of threats facing business and government.

Coviello's is a sentiment shared by multiple industry representatives at the conference, who said that the threat facing private and government networks called for a more unified response from all cybersecurity stakeholders.

The key to this happening is for vendors to stop viewing their technologies as "piecemeal" products aimed at addressing discrete security problems, Coviello said. Rather the emphasis needs to be on ensuring that each vendor's products works well with others' products to provide better information risk management opportunities, Coviello said.

Computerworld

Full Story :

• **RSA: The fundamental challenge of security versus privacy**

A fundamental tension exists in balancing individual privacy rights and the collective right to security, Gary McGraw, CTO of application security vendor Cigital, said at the RSA Conference on Tuesday.

"When you do something under FISA, you achieve a good balance," Joel said.

SC Magazine

Full Story :

<http://www.scmagazineus.com/RSA-The-fundamental-challenge-of-security-versus-privacy/article/131098/>

• **RSA: Cybercriminals keeping up with banking safeguards**

Threats are becoming more sophisticated, and cybercriminals are getting smarter at evading new authentication controls, according to an RSA Conference panel of security practitioners representing three major financial institutions.

Members of the panel, comprising experts at Bank of America, PayPal and JPMorganChase, agreed Wednesday that the burden is on them to secure their systems for customers -- many of whom are being greeted with slick new attempts to take over accounts. Securing systems includes implementing a defense-in-depth approach that offers multifactor authentication on the front end and fraud detection capabilities on the back end, the panelists said.

"The bad guys invested in a spell checker," joked David Shroyer, senior vice president at Bank of America's Online Security and Enrollment division. "I'd love to combat phishing in 2004 versus what we're facing today."

SC Magazine

Full Story :

<http://www.scmagazineus.com/RSA-Cybercriminals-keeping-up-with-banking-safeguards/article/131165/>

• **RSA: National consumer privacy and security law needed**

The question of whether the United States needs a national consumer data privacy and security law was met with a resounding "yes" from panelists on Wednesday at the RSA Conference.

The country is operating amid a fundamental paradox -- it has too many privacy and security laws and at the same time, too few, said panelist James Dempsey, policy director at the Center for Democracy and Technology, a nonprofit advocacy group.

Dempsey said the various federal laws securing credit reports, medical data, education records and credit cards are like a "patchwork quilt." He added that having it this way does not serve either consumers or the industry well.

SC Magazine

Full Story :

<http://www.scmagazineus.com/RSA-National-consumer-privacy-and-security-law-needed/article/131187/>

New Vulnerabilities Tested in SecureScout

• **18342 Internet Explorer Blended Threat Remote Code Execution Vulnerability (MS09-014/963027) (Remote File Checking)**

A blended threat remote code execution vulnerability exists in the way that Internet Explorer locates and opens files on the system. 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. 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.

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

References:

* MISC:

<http://aviv.rafton.net/2008/05/31/SafariPwnsInternetExplorer.aspx>

* MISC:

<http://blogs.zdnet.com/security/?p=1230>

* MISC:

http://www.dhanjani.com/archives/2008/05/safari_carpet_bomb.html

* MISC:

<http://www.microsoft.com/technet/security/advisory/953818.msp>

* APPLE: APPLE-SA-2008-06-19

<http://lists.apple.com/archives/security-announce/2008/Jun/msg00001.html>

* MS: MS09-015

<http://www.microsoft.com/technet/security/bulletin/ms09-015.msp>

* CERT: TA09-104A

<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>

* BID: 29445

<http://www.securityfocus.com/bid/29445>

* SECTrack: 1022047

<http://www.securitytracker.com/id?1022047>

* VUPEN: ADV-2008-1706

<http://www.frsirt.com/english/advisories/2008/1706>

* SECTrack: 1020150

<http://securitytracker.com/id?1020150>

* SECUNIA: 30467

<http://secunia.com/advisories/30467>

* VUPEN: ADV-2009-1028

<http://www.vupen.com/english/advisories/2009/1028>

* VUPEN: ADV-2009-1029

<http://www.vupen.com/english/advisories/2009/1029>

* XF: apple-safari-windows-code-execution(42765)

<http://xforce.iss.net/xforce/xfdb/42765>

CVE Reference:

CVE-2008-2540 (cve.mitre.org, nvd.nist.gov)

• 18343 Internet Explorer WinINET Credential Reflection Vulnerability (MS09-014/963027) (Remote File Checking)

A remote code execution vulnerability exists in the way that WinINET handles NTLM credentials when a user connects to an attacker's server by way of the HTTP protocol. This vulnerability allows an attacker to replay the user's credentials back to the attacker and to execute code in the context of the logged-on user. 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.

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

References:

* MS: MS09-013

<http://www.microsoft.com/technet/security/Bulletin/MS09-013.msp>

* MS: MS09-014

<http://www.microsoft.com/technet/security/Bulletin/MS09-014.msp>

* CERT: TA09-104A

<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>

* OSVDB: 53619

<http://osvdb.org/53619>

* SECTrack: 1022041

<http://www.securitytracker.com/id?1022041>

* SECUNIA: 34677

<http://secunia.com/advisories/34677>

* SECUNIA: 34678

<http://secunia.com/advisories/34678>

* VUPEN: ADV-2009-1027

<http://www.vupen.com/english/advisories/2009/1027>

* VUPEN: ADV-2009-1028

<http://www.vupen.com/english/advisories/2009/1028>

CVE Reference:

CVE-2009-0550 (cve.mitre.org, nvd.nist.gov)

• 18344 Internet Explorer Page Transition Memory Corruption Vulnerability (MS09-014/963027) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer handles transition when navigating between Web pages. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code if a user visited a specially crafted Web site. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * MS: MS09-014
<http://www.microsoft.com/technet/security/Bulletin/MS09-014.msp>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
- * OSVDB: 53624
<http://osvdb.org/53624>
- * SECTRAK: 1022042
<http://www.securitytracker.com/id?1022042>
- * SECUNIA: 34678
<http://secunia.com/advisories/34678>
- * VUPEN: ADV-2009-1028
<http://www.vupen.com/english/advisories/2009/1028>

CVE Reference:

CVE-2009-0551 (cve.mitre.org, nvd.nist.gov)

• 18345 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2009-0552) (MS09-014/963027) (Remote File Checking)

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

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

References:

- * MS: MS09-014
<http://www.microsoft.com/technet/security/Bulletin/MS09-014.msp>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
- * OSVDB: 53625
<http://osvdb.org/53625>
- * SECTRAK: 1022042
<http://www.securitytracker.com/id?1022042>
- * SECUNIA: 34678
<http://secunia.com/advisories/34678>
- * VUPEN: ADV-2009-1028
<http://www.vupen.com/english/advisories/2009/1028>

CVE Reference:

CVE-2009-0552 (cve.mitre.org, nvd.nist.gov)

• 18346 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2009-0553) (MS09-014/963027) (Remote File Checking)

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

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

References:

* MS: MS09-014
<http://www.microsoft.com/technet/security/Bulletin/MS09-014.msp>
* CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
* OSVDB: 53626
<http://osvdb.org/53626>
* SECTrack: 1022042
<http://www.securitytracker.com/id?1022042>
* SECUNIA: 34678
<http://secunia.com/advisories/34678>
* VUPEN: ADV-2009-1028
<http://www.vupen.com/english/advisories/2009/1028>

CVE Reference:

CVE-2009-0553 (cve.mitre.org, nvd.nist.gov)

• **18347 Internet Explorer Uninitialized Memory Corruption Vulnerability (CVE-2009-0554) (MS09-014/963027) (Remote File Checking)**

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

* MS: MS09-014
<http://www.microsoft.com/technet/security/Bulletin/MS09-014.msp>
* CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
* SECTrack: 1022042
<http://www.securitytracker.com/id?1022042>
* SECUNIA: 34678
<http://secunia.com/advisories/34678>
* VUPEN: ADV-2009-1028
<http://www.vupen.com/english/advisories/2009/1028>

CVE Reference:

CVE-2009-0554 (cve.mitre.org, nvd.nist.gov)

• **18348 Excel Memory Corruption Vulnerability (CVE-2009-0100) (MS09-009/968557) (Remote File Checking)**

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed object. 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: MS09-009
<http://www.microsoft.com/technet/security/Bulletin/MS09-009.msp>
* CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
* OSVDB: 53665
<http://osvdb.org/53665>
* SECTrack: 1022039
<http://www.securitytracker.com/id?1022039>

CVE Reference:

CVE-2009-0100 (cve.mitre.org, nvd.nist.gov)

• **18349 Excel Memory Corruption Vulnerability (CVE-2009-0238) (MS09-009/968557) (Remote File Checking)**

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed object. 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:

- * MISC:
<http://blogs.zdnet.com/security/?p=2658>
- * MISC:
<http://isc.sans.org/diary.html?storyid=5923>
- * MISC:
http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-022310-4202-99
- * CONFIRM:
<http://www.microsoft.com/technet/security/advisory/968272.msp>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
- * BID: 33870
<http://www.securityfocus.com/bid/33870>
- * SECTrack: 1021744
<http://securitytracker.com/id?1021744>
- * XF: ms-excel-unspecified-code-execution(48875)
<http://xforce.iss.net/xforce/xfdb/48875>
- * MS: MS09-009
<http://www.microsoft.com/technet/security/Bulletin/MS09-009.msp>

CVE Reference:

CVE-2009-0238 (cve.mitre.org, nvd.nist.gov)

• 18350 Windows HTTP Services Integer Underflow Vulnerability (MS09-013/960803) (Remote File Checking)

A remote code execution vulnerability exists in the way that Windows HTTP Services handle specific values that are returned by a remote Web server. 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 the same user rights as the service or application which calls the WinHTTP API to connect to the attacker's Web server.

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

References:

- * MS: MS09-013
<http://www.microsoft.com/technet/security/Bulletin/MS09-013.msp>
- * CERT: TA09-104A
<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>
- * OSVDB: 53620
<http://osvdb.org/53620>
- * SECTrack: 1022041
<http://www.securitytracker.com/id?1022041>
- * SECUNIA: 34677
<http://secunia.com/advisories/34677>
- * VUPEN: ADV-2009-1027
<http://www.vupen.com/english/advisories/2009/1027>

CVE Reference:

CVE-2009-0086 (cve.mitre.org, nvd.nist.gov)

• 18351 Windows HTTP Services Certificate Name Mismatch Vulnerability (MS09-013/960803) (Remote File Checking)

A spoofing vulnerability exists in Windows HTTP Services as a result of the incomplete validation of the distinguished name in a digital certificate. When combined with specific other attacks, such as DNS spoofing, this may allow an attacker to successfully spoof the digital certificate of a Web site for any application that uses Windows HTTP Services.

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

References:

- * MS: MS09-013
<http://www.microsoft.com/technet/security/Bulletin/MS09-013.msp>
- * CERT: TA09-104A

<http://www.us-cert.gov/cas/techalerts/TA09-104A.html>

* BID: 34437

<http://www.securityfocus.com/bid/34437>

* SECTRACK: 1022041

<http://www.securitytracker.com/id?1022041>

* SECUNIA: 34677

<http://secunia.com/advisories/34677>

* VUPEN: ADV-2009-1027

<http://www.vupen.com/english/advisories/2009/1027>

CVE Reference:

CVE-2009-0089 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-0718 HP CVSS 2.0 Score = 10.0

Unspecified vulnerability in HP StorageWorks Storage Mirroring 5 before 5.1.1.1090.15 allows remote attackers to execute arbitrary code via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=124025929213175&w=2>

HP: <http://marc.info/?l=bugtraq&m=124025929213175&w=2>

CVE Reference: [CVE-2009-0718](#)

• CVE-2009-0716 HP CVSS 2.0 Score = 7.5

Unspecified vulnerability in HP StorageWorks Storage Mirroring 5 before 5.1.1.1090.15 allows remote attackers to cause a denial of service or obtain "access" via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=124025929213175&w=2>

HP: <http://marc.info/?l=bugtraq&m=124025929213175&w=2>

CVE Reference: [CVE-2009-0716](#)

• CVE-2009-0715 HP CVSS 2.0 Score = 6.5

Unspecified vulnerability in Secure NaviCLI in HP Storage Essentials 6.0.2 through 6.0.4 allows remote authenticated users to obtain "access" or "extended privileges" via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=124025839111157&w=2>

CVE Reference: [CVE-2009-0715](#)

• CVE-2009-0717 HP CVSS 2.0 Score = 5.0

Unspecified vulnerability in HP StorageWorks Storage Mirroring 5 before 5.1.1.1090.15 allows remote attackers to cause a denial of service via unknown vectors.

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

References:

HP: <http://marc.info/?l=bugtraq&m=124025929213175&w=2>

CVE Reference: [CVE-2009-0717](#)

• CVE-2009-1355 IBM CVSS 2.0 Score = 7.2

Stack-based buffer overflow in muxatmd in IBM AIX 5.2, 5.3, and 6.1 allows local users to gain privileges via a long filename.

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

References:

VUPEN: <http://www.vupen.com/english/advisories/2009/1056>
BID: <http://www.securityfocus.com/bid/34543>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ48562>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ48561>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ48502>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ48501>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ48500>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ48499>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ48496>
AIXAPAR: <http://www.ibm.com/support/docview.wss?uid=isg1IZ48495>
SECUNIA: <http://secunia.com/advisories/34662>
IDFENSE: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=784>
CONFIRM: http://aix.software.ibm.com/aix/efixes/security/muxatmd_advisory.asc

CVE Reference: [CVE-2009-1355](#)

• CVE-2009-1350 Novell CVSS 2.0 Score = 10.0

Unspecified vulnerability in xtagent.exe in Novell NetIdentity Client before 1.2.4 allows remote attackers to execute arbitrary code by establishing an IPC\$ connection to the XTIERRPCPIPE named pipe, and sending RPC messages that trigger a dereference of an arbitrary pointer.

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

References:

MISC: <http://www.zerodayinitiative.com/advisories/ZDI-09-016/>
VUPEN: <http://www.vupen.com/english/advisories/2009/0954>
CONFIRM: <http://download.novell.com/Download?buildid=6ERQGPjRZ8o~>
MISC: https://bugzilla.novell.com/show_bug.cgi?id=437511
SECTRAK: <http://www.securitytracker.com/id?1021990>
BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/502514/100/0/threaded>

CVE Reference: [CVE-2009-1350](#)

• CVE-2009-1360 Linux CVSS 2.0 Score = 7.1

The `__inet6_check_established` function in `net/ipv6/inet6_hashtables.c` in the Linux kernel before 2.6.29, when Network Namespace Support (aka `NET_NS`) is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via vectors involving IPv6 packets.

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

References:

CONFIRM: <http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.29>
CONFIRM: <http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=3f53a38131a4e7a053c0aa060aba0411242fb6b9>

MISC: http://xorl.wordpress.com/2009/04/21/linux-kernel-net_ns-ipv6-null-pointer-dereference/

BID: <http://www.securityfocus.com/bid/34602>

CVE Reference: [CVE-2009-1360](#)

• **CVE-2009-0195 Apple CVSS 2.0 Score = 6.8**

Heap-based buffer overflow in Xpdf 3.02pl2 and earlier, CUPS 1.3.9, and probably other products, allows remote attackers to execute arbitrary code via a PDF file with crafted JBIG2 symbol dictionary segments.

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

References:

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/502762/100/0/threaded>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/502759/100/0/threaded>

MISC: http://secunia.com/secunia_research/2009-18/

MISC: http://secunia.com/secunia_research/2009-17/

CVE Reference: [CVE-2009-0195](#)

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