netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 9

February 29, 2008

Table of Contents

Product Focus

Spida Digispid Worm Scanner – The 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).

This Week in Review

Some advice to the lawmakers. Now we need to protect our cell phones. A look at faulty security policies. Bypassing disk encryption maybe not that easy.

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

- **Four laws Congress needs to pass now to boost computer security**

Even though we have a new Congress, I doubt that much will change with regard to computer security. While a law related to identity theft will probably be passed in one form or another, I expect that it will be trivial and not deal with preventing the theft of individuals' personal information. Corporate lobbyists have proved themselves to be too adept at manipulating members of Congress so they don't pass laws requiring companies to be proactive, especially with regard to security measures.

Identity theft is a symptom of poor computer security. There are two underlying methods of identity theft: hacks of vendor computers, and client-side attacks. Vendor hacks are the result of poor security on the part of the vendor and often lead to the theft of thousands, or millions, of credit card numbers, at once. The laws passed in this regard basically state requirements that vendors have to follow once data is stolen.

computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9009984

❖ Wiretapping Made Easy

Silently tapping into a private cellphone conversation is no longer a high-tech trick reserved for spies and the FBI. Thanks to the work of two young cyber-security researchers, cellular snooping may soon be affordable enough for your next-door neighbor.

In a presentation Wednesday at the Black Hat security conference in Washington, D.C., David Hulton and Steve Muller demonstrated a new technique for cracking the encryption used to prevent eavesdropping on global system for mobile communications (GSM) cellular signals, the type of radio frequency coding used by major cellular service providers including AT&T (nyse: T - news - people), Cingular and T-Mobile. Combined with a radio receiver, the pair say their technique allows an eavesdropper to record a conversation on these networks from miles away and decode it in about half an hour with just $1,000 in computer storage and processing equipment.

forbes

Full Story :
http://www.forbes.com/home/security/2008/02/21/cellular-spying-decryption-tech-security-cx_ag_0221cellular.html

❖ Five basic mistakes of security policy

TKAs I mentioned in my last article, security policies serve to protect (data, customers, employees, technological systems), define (the company's stance on security), and minimize risk (internal and external exposure and publicity fallout in the event of a breach). Security policy creation and dissemination are not just a good idea; both are mandated by a slew of corporate regulations, including PCI, HIPAA, and FISMA.

This story presents five mistakes that companies commonly make when writing and implementing security policies. As simplistic as some of these errors sound, they happen often enough and cause heavy damage to companies' bottom lines.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9065202&intsrc=hm_list

- **Cold bits as a security bypass**

Bypassing disk encryption with a spray can
Network World's headline was certainly designed to catch a security person's eye: "Disk encryption easily cracked, researchers find." In most cases, however, the risk, while real, is less than the headline implies.
It turns out that some researchers at Princeton University followed up on earlier research showing that modern computer memories retained their contents even with the power off (known as memory remanence), and that the retention time could be lengthened by cooling the memory. (See the chapter on physical tamper resistance in Ross Anderson's Security Engineering: A Guide to Building Dependable Distributed Systems.

Network world

Full Story :
http://www.networkworld.com/columnists/2008/022608-bradner.html?fsrc=rss-columns

New Vulnerabilities Tested in SecureScout

- **16868 Microsoft Excel File Handling Code Execution (Remote File Checking)**

Unspecified vulnerability in Microsoft Excel 2004 and earlier, and Microsoft Office Excel Viewer 2003, allows remote attackers to execute arbitrary code via an Excel file with a malformed header, which triggers memory corruption.

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

References:

* MSKB: 947563
http://www.microsoft.com/technet/security/advisory/947563.mspx
* BID: 27305
http://www.securityfocus.com/bid/27305
* FRSIRT: ADV-2008-0146
http://www.frsirt.com/english/advisories/2008/0146
* SECTRACK: 1019200
http://securitytracker.com/id?1019200
* SECUNIA: 28506
http://secunia.com/advisories/28506
* XF: microsoft-excel-unspecified-code-execution(39699)
http://xforce.iss.net/xforce/xfdb/39699

CVE Reference: CVE-2008-0081

❖ 16867 BIND buffer overflow in inet_network()

An off-by-one error in the inet_network() function in libbind could lead to memory corruption with certain inputs.

Applications linked against libbind which call inet_network() with untrusted inputs could lead to a denial-of-service or potentially code execution.

Note that none of the applications shipped with BIND 8 or BIND 9 call inet_network().

The vulnerability has been fixed in versions 9.3.5, 9.4.3, 9.5.0b2.

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

References:

* BUGTRAQ: 20080124 rPSA-2008-0029-1 bind bind-utils
http://www.securityfocus.com/archive/1/archive/1/487000/100/0/threaded
* CONFIRM:
http://www.isc.org/index.pl?/sw/bind/bind-security.php
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=429149
* CONFIRM:
https://issues.rpath.com/browse/RPL-2169
* FEDORA: FEDORA-2008-0903
https://www.redhat.com/archives/fedora-package-announce/2008-January/msg00781.html
* FEDORA: FEDORA-2008-0904
https://www.redhat.com/archives/fedora-package-announce/2008-January/msg00782.html
* FREEBSD: FreeBSD-SA-08:02
http://security.freebsd.org/advisories/FreeBSD-SA-08:02.libc.asc
* CERT-VN: VU#203611
http://www.kb.cert.org/vuls/id/203611
* BID: 27283
http://www.securityfocus.com/bid/27283
* FRSIRT: ADV-2008-0193
http://www.frsirt.com/english/advisories/2008/0193
* SECTRACK: 1019189
http://www.securitytracker.com/id?1019189
* SECUNIA: 28367
http://secunia.com/advisories/28367
* SECUNIA: 28579
http://secunia.com/advisories/28579
* SECUNIA: 28487
http://secunia.com/advisories/28487
* SECUNIA: 28429
http://secunia.com/advisories/28429
* XF: freebsd-inetnetwork-bo(39670)
http://xforce.iss.net/xforce/xfdb/39670

CVE Reference: CVE-2008-0122

❖ 14495 Adobe Acrobat / Reader printSepsWithParams integer overflow Vulnerability (Remote File Checking)

Integer overflow in Adobe Reader and Acrobat 8.1.1 and earlier allows remote attackers to execute arbitrary code via crafted arguments to the printSepsWithParams, which triggers memory corruption.

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

References:

* BUGTRAQ: 20080211 ZDI-08-004: Adobe AcrobatReader Javascript for PDF Integer Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/488000/100/0/threaded
* MISC:
http://www.zerodayinitiative.com/advisories/ZDI-08-004.html
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa08-01.html
* REDHAT: RHSA-2008:0144
http://www.redhat.com/support/errata/RHSA-2008-0144.html
* SUSE: SUSE-SA:2008:009
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00007.html
* SECUNIA: 28983
http://secunia.com/advisories/28983
* SECUNIA: 29065
http://secunia.com/advisories/29065

CVE Reference: CVE-2008-0726

❖ 14494 Adobe Acrobat / Reader DOC.print function Vulnerability (Remote File Checking)

The DOC.print function in the Adobe JavaScript API, as used by Adobe Acrobat and Reader before 8.1.2, allows remote attackers to configure silent non-interactive printing, and trigger the printing of an arbitrary number of copies of a document.

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

References:

* BUGTRAQ: 20080208 Adobe Reader/Acrobat Remote PDF Print Silently Vulnerability
http://www.securityfocus.com/archive/1/archive/1/487760/100/0/threaded
* MISC:
http://kb.adobe.com/selfservice/viewContent.do?externalId=kb403079&sliceId=1
* MISC:
http://www.fortiguardcenter.com/advisory/FGA-2008-04.html
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa08-01.html

* REDHAT: RHSA-2008:0144
http://www.redhat.com/support/errata/RHSA-2008-0144.html
* SUSE: SUSE-SA:2008:009
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00007.html
* CERT: TA08-043A
http://www.us-cert.gov/cas/techalerts/TA08-043A.html
* BID: 27641
http://www.securityfocus.com/bid/27641
* FRSIRT: ADV-2008-0425
http://www.frsirt.com/english/advisories/2008/0425/references
* SECUNIA: 28802
http://secunia.com/advisories/28802
* SECUNIA: 28851
http://secunia.com/advisories/28851
* SECUNIA: 28983
http://secunia.com/advisories/28983
* SECUNIA: 29065
http://secunia.com/advisories/29065

CVE Reference: CVE-2008-0667

❖ 14493 Adobe Acrobat / Reader multiple unspecified vulnerabilities (Remote File Checking)

Multiple unspecified vulnerabilities in Adobe Reader and Acrobat before 8.1.2 have unknown impact and attack vectors.

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

References:

* CONFIRM:
http://kb.adobe.com/selfservice/viewContent.do?externalId=kb403079&sliceId=1
* CONFIRM:
http://blogs.adobe.com/acroread/2008/02/adobe_reader_812_for_linux_and.html
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa08-01.html
* REDHAT: RHSA-2008:0144
http://www.redhat.com/support/errata/RHSA-2008-0144.html
* SUSE: SUSE-SA:2008:009
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00007.html
* CERT: TA08-043A
http://www.us-cert.gov/cas/techalerts/TA08-043A.html
* BID: 27641
http://www.securityfocus.com/bid/27641
* FRSIRT: ADV-2008-0425
http://www.frsirt.com/english/advisories/2008/0425
* SECTRACK: 1019346
http://securitytracker.com/id?1019346
* SECUNIA: 28802

http://secunia.com/advisories/28802
* SECUNIA: 28851
http://secunia.com/advisories/28851
* SECUNIA: 28983
http://secunia.com/advisories/28983
* SECUNIA: 29065
http://secunia.com/advisories/29065

CVE Reference: CVE-2008-0655

❖ 14492 Adobe Acrobat / Reader Untrusted search path vulnerability (Remote File Checking)

Untrusted search path vulnerability in Adobe Reader and Acrobat 8.1.1 and earlier allows local users to execute arbitrary code via a malicious Security Provider library in the reader's current working directory.

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

References:

* IDEFENSE: 20080208 Adobe Reader Security Provider Unsafe Libary Path Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=655
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa08-01.html
* REDHAT: RHSA-2008:0144
http://www.redhat.com/support/errata/RHSA-2008-0144.html
* CERT: TA08-043A
http://www.us-cert.gov/cas/techalerts/TA08-043A.html
* SECUNIA: 29065
http://secunia.com/advisories/29065

CVE Reference: CVE-2007-5666

❖ 14491 Adobe Acrobat / Reader arbitrary code execution via a crafted PDF Vulnerability (Remote File Checking)

Adobe Reader and Acrobat 8.1.1 and earlier allow remote attackers to execute arbitrary code via a crafted PDF file that calls an insecure JavaScript method in the EScript.api plug-in.

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

References:

* IDEFENSE: 20080208 Adobe Reader and Acrobat JavaScript Insecure Method Exposure Vulnerability
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=656
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa08-01.html
* REDHAT: RHSA-2008:0144

http://www.redhat.com/support/errata/RHSA-2008-0144.html
* CERT: TA08-043A
http://www.us-cert.gov/cas/techalerts/TA08-043A.html
* CERT-VN: VU#140129
http://www.kb.cert.org/vuls/id/140129
* SECUNIA: 29065
http://secunia.com/advisories/29065

CVE Reference: CVE-2007-5663

❖ 14490 Adobe Acrobat / Reader multiple buffer overflows Vulnerabilities (Remote File Checking)

Multiple buffer overflows in Adobe Reader and Acrobat 8.1.1 and earlier allow remote attackers to execute arbitrary code via a PDF file with long arguments to unspecified JavaScript methods.

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

References:

* IDEFENSE: 20080208 Adobe Reader and Acrobat Multiple Stack-based Buffer Overflow Vulnerabilities
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=657
* CONFIRM:
http://www.adobe.com/support/security/advisories/apsa08-01.html
* REDHAT: RHSA-2008:0144
http://www.redhat.com/support/errata/RHSA-2008-0144.html
* CERT: TA08-043A
http://www.us-cert.gov/cas/techalerts/TA08-043A.html
* CERT-VN: VU#666281
http://www.kb.cert.org/vuls/id/666281
* SECUNIA: 29065
http://secunia.com/advisories/29065

CVE Reference: CVE-2007-5659

❖ 16729 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS08)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html

* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)
http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3710

❖ 16728 Oracle Application Server - OC4J component unspecified Vulnerability (jul-2006/AS07)

An unspecified vulnerability with unknown impact exists in Oracle Application Server OC4J component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2006.html
* MISC:
http://www.red-database-security.com/advisory/oracle_cpu_july_2006.html
* HP: HPSBMA02133
http://www.securityfocus.com/archive/1/archive/1/440758/100/100/threaded
* CERT: TA06-200A
http://www.us-cert.gov/cas/techalerts/TA06-200A.html
* BID: 19054
http://www.securityfocus.com/bid/19054
* FRSIRT: ADV-2006-2863
http://www.frsirt.com/english/advisories/2006/2863
* FRSIRT: ADV-2006-2947
http://www.frsirt.com/english/advisories/2006/2947
* SECTRACK: 1016529
http://securitytracker.com/id?1016529
* SECUNIA: 21111
http://secunia.com/advisories/21111
* SECUNIA: 21165
http://secunia.com/advisories/21165
* XF: oracle-cpu-july-2006(27897)

http://xforce.iss.net/xforce/xfdb/27897

CVE Reference: CVE-2006-3712

New Vulnerabilities found this Week

Mozilla Thunderbird MIME Processing Buffer Overflow Vulnerability

"Heap-based buffer overflow; Execution of arbitrary code"

A vulnerability has been reported in Mozilla Thunderbird, which can be exploited by malicious people to potentially compromise a user's system.

The vulnerability is caused due to an error within the handling of external-body MIME types. This can be exploited to cause a heap-based buffer overflow with three bytes by tricking a user into viewing a specially crafted email.

Successful exploitation may allow execution of arbitrary code.

The vulnerability is reported in version 2.0.0.9. Prior versions may also be affected.

References:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=668
http://www.mozilla.org/security/announce/2008/mfsa2008-12.html

Symantec Products Symantec Decomposer RAR File Handling Vulnerabilities

"Denial of Service; Execution of arbitrary code"

Two vulnerabilities have been reported in various Symantec products, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system.

1) A boundary error in Symantec's Decomposer engine can be exploited to cause a stack-based buffer overflow when handling a specially crafted .RAR file.

Successful exploitation allows execution of arbitrary code.

2) An error in Symantec's Decomposer engine can be exploited to cause the process to consume large amounts of memory when handling a specially crafted .RAR file.

References:
http://www.symantec.com/avcenter/security/Content/2008.02.27.html

Apple Mac OS X "ipcomp6_input()" Denial of Service

"Denial of Service"

A vulnerability has been reported in Apple Mac OS X, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the "ipcomp6_input()" function in bsd/netinet6/ipcomp_input.c when processing IPv6 packets with an IPComp header. This

can be exploited to crash a vulnerable system by sending a specially crafted IPv6 packet.

The vulnerability is reported in Mac OS X 10.5.1 and 10.5.2. Other versions may also be affected.

References:
http://www.digit-labs.org/files/exploits/xnu-ipv6-ipcomp.c

ISS Internet Scanner Reporting Engine Script Insertion Vulnerability
"Script insertion attacks"

A vulnerability has been reported in ISS Internet Scanner, which can be exploited by malicious people to conduct script insertion attacks.

Input passed via unspecified parameters is not properly sanitized before being saved as an HTML report. This can be exploited to insert arbitrary HTML and script code, which is executed in a user's browser session when the malicious data is viewed.

The vulnerability is reported in version 7.0 Service Pack 2 (build 7.2.2005.52). Other versions may also be affected.

References:
http://jvn.jp/jp/JVN%2342381549/index.html

VMware Products Shared Folders Directory Traversal Vulnerability
"Read or write arbitrary files on the host OS via directory traversal attacks"

Gerardo Richarte has reported a vulnerability in VMware products, which can be exploited by malicious, local users or malicious applications to bypass certain security restrictions.

The vulnerability is caused due to an input validation error when handling pathnames within a shared folder in a guest OS. This can be exploited to e.g. read or write arbitrary files on the host OS via directory traversal attacks.

Successful exploitation requires that the shared folders feature is enabled with at least one folder configured for sharing between host and guest.

References:
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004034
http://lists.grok.org.uk/pipermail/full-disclosure/2008-February/060457.html

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