ScoutNews
The weekly Security update from the makers of SecureScout
September 04, 2009

2009 Issue #36

Table of Contents

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

Were the predictions correct? Bank gets sued for lax security. Cloud interoperability management needed. Opinion: SQL injections ought to have been eradicated.

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

- **Internet Security Trends 2009: An Interim Update**

CSO - The effects of cybercrime are far reaching. It would be a difficult task to find someone who has never been affected by malicious Internet activity, or who does not at the very least know someone who has been negatively impacted by cybercriminals. Advances in Internet technology and services continue to open up innumerable opportunities for learning, networking and increasing productivity. However, malware authors, spammers and phishers are also rapidly adopting new and varied attack vectors. If the Internet is to become a safer place, it is imperative to understand the trends and developments taking place in the Internet threat landscape and maintain online security best practices.

In December 2008, Symantec researchers predicted a number of security trends to watch out for in 2009. Now that we are into the second half of the year, it's time to check in on those predictions to see not only how they have panned out, but also what other developments have occurred. What follows is an update on the predictions Symantec made late last year, as well as a few new trends that our analysts have seen develop in the first half of 2009. Computerworld

Full Story :

http://www.computerworld.com/s/article/9137444/Internet_Security_Trends_2009_An_Interim_Update?source=rss_s

- **Court allows suit against bank for lax security**

Computerworld - A couple whose bank account was breached can sue their bank for its alleged failure to implement the latest security measures designed to prevent such compromises.

In a ruling issued last month, Judge Rebecca Pallmeyer, of the District Court for the Northern District of Illinois, denied a request by Citizens Financial Bank to dismiss a negligence claim brought against it by Marsha and Michael Shames-Yeakel. The Crown Point, Ind. couple -- customers of the bank -- alleged that Citizens' failure to implement up-to-date user authentication measures resulted in the theft of more than $26,000 from their home equity line of credit. Computerworld

Full Story :
http://www.computerworld.com/s/article/9137451/Court_allows_suit_against_bank_for_lax_security?source=rss_sec

- **Cloud interoperability on the horizon?**

Arguments for and against the cloud are starting to calm down a bit, and most people agree that the cloud is somewhere in your future, if not in your present.

Instead of arguing semantics of application development and delivery, the discussion should really be around how to deal with a mix of on-premise and on-demand, a combination that is unlikely to change in the foreseeable future.

I spent the first half of this week in Las Vegas at a nontech trade show, and missed both VMworld and the Red Hat Summit. However, watching and reading from afar, I noticed two major themes in discussion around both cloud computing and virtualization: cloud interoperability and the lack of application management tools. Cnet Security

Full Story :
http://news.cnet.com/8301-13846_3-10344713-62.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Opinion: No more excuses for SQL injection attacks**

Computerworld - We should have eradicated SQL injection attacks by now. SQL injection should be the Internet generation's smallpox or polio -- gone for good. Countermeasures are readily available and understood. They're easy to implement. And yet, I keep seeing headlines like "Huge Web hack attack infects 500,000 pages."

SQL injection attacks continue to be among the most fruitful against Web sites and applications. And why not? From an attacker's perspective, the database behind many Web applications is where the really juicy targets live. That's where you'll find customer records, credit card numbers and other good stuff.

And now attackers have started using SQL injection to plant malware on Web sites, so that visitors to those sites get their computers infected with the malware. The databases aren't just where the juicy targets are; they're ripe for planting malicious data that infects other people's computers. Computerworld

Full Story :
http://www.computerworld.com/s/article/9137478/Opinion_No_more_excuses_for_SQL_injection_attacks?source=rs

New Vulnerabilities Tested in SecureScout

- **18248 PHP 'chdir()' and 'ftok()' multiple safe_mode bypass Vulnerabilities**

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.

This has been reported in versions 5.x lower than 5.2.7.
Other versions may also be affected.

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

References:

* SREASONRES: 20080617 PHP 5.2.6 chdir(),ftok() (standard ext) safe_mode bypass
http://securityreason.com/achievement_securityalert/55
* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl
http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded
* CONFIRM:

http://wiki.rpath.com/Advisories:rPSA-2009-0035
* CONFIRM:
http://support.apple.com/kb/HT3549
* APPLE: APPLE-SA-2009-05-12
http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
* HP: HPSBUX02431
http://marc.info/?l=bugtraq&m=124654546101607&w=2
* CERT: TA09-133A
http://www.us-cert.gov/cas/techalerts/TA09-133A.html
* BID: 29796
http://www.securityfocus.com/bid/29796
* SECTRACK: 1020328
http://www.securitytracker.com/id?1020328
* SECUNIA: 35074
http://secunia.com/advisories/35074
* SECUNIA: 35650
http://secunia.com/advisories/35650
* SREASON: 3942
http://securityreason.com/securityalert/3942
* VUPEN: ADV-2009-1297
http://www.vupen.com/english/advisories/2009/1297
* XF: php-chdir-ftoc-security-bypass(43198)
http://xforce.iss.net/xforce/xfdb/43198

CVE Reference:

CVE-2008-2666 (cve.mitre.org, nvd.nist.gov)

• 18492 Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability (cisco-sa-20090325-udp)

Unspecified vulnerability in Cisco IOS 12.0 through 12.4, when configured with (1) IP Service Level Agreements (SLAs) Responder, (2) Session Initiation Protocol (SIP), (3) H.323 Annex E Call Signaling Transport, or (4) Media Gateway Control Protocol (MGCP) allows remote attackers to cause a denial of service (blocked input queue on the inbound interface) via a crafted UDP packet.

This vulnerability is documented in Cisco Bug ID CSCsk64158.

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

References:

* CONFIRM:
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml
* CISCO: 20090325 Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90426.shtml
* BID: 34245
http://www.securityfocus.com/bid/34245
* SECTRACK: 1021904
http://www.securitytracker.com/id?1021904
* XF: ios-udp-dos(49419)
http://xforce.iss.net/xforce/xfdb/49419

CVE Reference:

CVE-2009-0631 (cve.mitre.org, nvd.nist.gov)

• 18493 Cisco IOS Software WebVPN and SSLVPN Vulnerabilities (cisco-sa-20090325-webvpn) (CVE-2009-0626)

The SSLVPN feature in Cisco IOS 12.3 through 12.4 allows remote attackers to cause a denial of service (device reload or hang) via a crafted HTTPS packet.

This vulnerability is documented in Cisco Bug ID CSCsk62253.

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

References:

* CONFIRM:
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml
* CISCO: 20090325 Cisco IOS Software WebVPN and SSLVPN Vulnerabilities
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90424.shtml

* BID: 34239
http://www.securityfocus.com/bid/34239
* SECTRACK: 1021896
http://securitytracker.com/id?1021896
* SECUNIA: 34438
http://secunia.com/advisories/34438
* VUPEN: ADV-2009-0851
http://www.vupen.com/english/advisories/2009/0851
* XF: ios-sslvpn-dos(49425)
http://xforce.iss.net/xforce/xfdb/49425

CVE Reference:

CVE-2009-0626 (cve.mitre.org, nvd.nist.gov)

• 18494 Cisco IOS Software WebVPN and SSLVPN Vulnerabilities (cisco-sa-20090325-webvpn) (CVE-2009-0628)

Memory leak in the SSLVPN feature in Cisco IOS 12.3 through 12.4 allows remote attackers to cause a denial of service (memory consumption and device crash) by disconnecting an SSL session in an abnormal manner, leading to a Transmission Control Block (TCB) leak.

This vulnerability is documented in Cisco Bug ID CSCsw24700.

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

References:

* CONFIRM:
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml
* CISCO: 20090325 Cisco IOS Software WebVPN and SSLVPN Vulnerabilities
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90424.shtml
* BID: 34239
http://www.securityfocus.com/bid/34239
* SECTRACK: 1021896
http://securitytracker.com/id?1021896
* SECUNIA: 34438
http://secunia.com/advisories/34438
* VUPEN: ADV-2009-0851
http://www.vupen.com/english/advisories/2009/0851
* XF: ios-sslvpn-tcbleak-dos(49427)
http://xforce.iss.net/xforce/xfdb/49427

CVE Reference:

CVE-2009-0628 (cve.mitre.org, nvd.nist.gov)

• 18495 Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability (cisco-sa-20090325-tcp)

The (1) Airline Product Set (aka ALPS), (2) Serial Tunnel Code (aka STUN), (3) Block Serial Tunnel Code (aka BSTUN), (4) Native Client Interface Architecture (NCIA) support, (5) Data-link switching (aka DLSw), (6) Remote Source-Route Bridging (RSRB), (7) Point to Point Tunneling Protocol (PPTP), (8) X.25 for Record Boundary Preservation (RBP), (9) X.25 over TCP (XOT), and (10) X.25 Routing features in Cisco IOS 12.2 and 12.4 allows remote attackers to cause a denial of service (device reload) via a series of crafted TCP packets.

This vulnerability is documented in Cisco Bug ID CSCsr29468.

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

References:

* CONFIRM:
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a90469.shtml
* CISCO: 20090325 Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a904cb.shtml
* BID: 34238
http://www.securityfocus.com/bid/34238
* SECTRACK: 1021903
http://securitytracker.com/id?1021903
* SECUNIA: 34438
http://secunia.com/advisories/34438
* VUPEN: ADV-2009-0851

http://www.vupen.com/english/advisories/2009/0851
* XF: ios-tcp-dos(49420)
http://xforce.iss.net/xforce/xfdb/49420

CVE Reference:

CVE-2009-0629 (cve.mitre.org, nvd.nist.gov)

• 18496 Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities (cisco-sa-20090729-bgp) (CVE-2009-1168)

Cisco IOS 12.0(32)S12 through 12.0(32)S13 and 12.0(33)S3 through 12.0(33)S4, 12.0(32)SY8 through 12.0(32)SY9, 12.2(33)SXI1, 12.2XNC before 12.2(33)XNC2, 12.2XND before 12.2(33)XND1, and 12.4(24)T1; and IOS XE 2.3 through 2.3.1t and 2.4 through 2.4.0; when RFC4893 BGP routing is enabled, allows remote attackers to cause a denial of service (memory corruption and device reload) by using an RFC4271 peer to send an update with a long series of AS numbers.

This vulnerability is documented in Cisco Bug ID CSCsy86021.

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

References:

* CISCO: 20090729 Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities
http://www.cisco.com/en/US/products/products_security_advisory09186a0080aea4c9.shtml
* BID: 35862
http://www.securityfocus.com/bid/35862
* SECTRACK: 1022619
http://www.securitytracker.com/id?1022619
* SECUNIA: 36046
http://secunia.com/advisories/36046
* VUPEN: ADV-2009-2082
http://www.vupen.com/english/advisories/2009/2082

CVE Reference:

CVE-2009-1168 (cve.mitre.org, nvd.nist.gov)

• 18497 Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities (cisco-sa-20090729-bgp) (CVE-2009-2049)

Cisco IOS 12.0(32)S12 through 12.0(32)S13 and 12.0(33)S3 through 12.0(33)S4, 12.0(32)SY8 through 12.0(32)SY9, 12.2(33)SXI1 through 12.2(33)SXI2, 12.2XNC before 12.2(33)XNC2, 12.2XND before 12.2(33)XND1, and 12.4(24)T1; and IOS XE 2.3 through 2.3.1t and 2.4 through 2.4.0; when RFC4893 BGP routing is enabled, allows remote attackers to cause a denial of service (device reload) by using an RFC4271 peer to send a malformed update.

This vulnerability is documented in Cisco Bug ID CSCta33973.

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

References:

* CISCO: 20090729 Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities
http://www.cisco.com/en/US/products/products_security_advisory09186a0080aea4c9.shtml
* BID: 35860
http://www.securityfocus.com/bid/35860
* SECTRACK: 1022619
http://www.securitytracker.com/id?1022619
* SECUNIA: 36046
http://secunia.com/advisories/36046
* VUPEN: ADV-2009-2082
http://www.vupen.com/english/advisories/2009/2082

CVE Reference:

CVE-2009-2049 (cve.mitre.org, nvd.nist.gov)

• 18498 PHP PCRE Heap-based buffer overflow Vulnerability

Heap-based buffer overflow in pcre_compile.c in the Perl-Compatible Regular Expression (PCRE) library 7.7 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a regular expression that begins with an option and contains multiple branches.

This has been reported in versions 5.x lower than 5.2.7.

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

References:

* BUGTRAQ: 20081027 rPSA-2008-0305-1 pcre
http://www.securityfocus.com/archive/1/archive/1/497828/100/0/threaded
* CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=228091
* CONFIRM:
http://ftp.gnome.org/pub/GNOME/sources/glib/2.16/glib-2.16.4.changes
* CONFIRM:
http://support.apple.com/kb/HT3216
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0305
* CONFIRM:
http://support.apple.com/kb/HT3549
* APPLE: APPLE-SA-2008-10-09
http://lists.apple.com/archives/security-announce/2008/Oct/msg00001.html
* APPLE: APPLE-SA-2009-05-12
http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
* DEBIAN: DSA-1602
http://www.debian.org/security/2008/dsa-1602
* FEDORA: FEDORA-2008-6025
https://www.redhat.com/archives/fedora-package-announce/2008-July/msg00105.html
* FEDORA: FEDORA-2008-6048
https://www.redhat.com/archives/fedora-package-announce/2008-July/msg00123.html
* GENTOO: GLSA-200807-03
http://www.gentoo.org/security/en/glsa/glsa-200807-03.xml
* HP: HPSBUX02431
http://marc.info/?l=bugtraq&m=124654546101607&w=2
* MANDRIVA: MDVSA-2008:147
http://www.mandriva.com/security/advisories?name=MDVSA-2008:147
* MANDRIVA: MDVSA-2009:023
http://www.mandriva.com/security/advisories?name=MDVSA-2009:023
* SUSE: SUSE-SR:2008:014
http://lists.opensuse.org/opensuse-security-announce/2008-07/msg00001.html
* UBUNTU: USN-624-1
http://www.ubuntu.com/usn/usn-624-1
* UBUNTU: USN-628-1
http://www.ubuntu.com/usn/usn-628-1
* CERT: TA09-133A
http://www.us-cert.gov/cas/techalerts/TA09-133A.html
* BID: 30087
http://www.securityfocus.com/bid/30087
* BID: 31681
http://www.securityfocus.com/bid/31681
* SECUNIA: 35074
http://secunia.com/advisories/35074
* SECUNIA: 35650
http://secunia.com/advisories/35650
* VUPEN: ADV-2008-2005
http://www.frsirt.com/english/advisories/2008/2005
* VUPEN: ADV-2008-2006
http://www.frsirt.com/english/advisories/2008/2006
* VUPEN: ADV-2008-2780
http://www.frsirt.com/english/advisories/2008/2780
* SECUNIA: 30916
http://secunia.com/advisories/30916
* SECUNIA: 30944
http://secunia.com/advisories/30944
* SECUNIA: 30958
http://secunia.com/advisories/30958
* SECUNIA: 30961
http://secunia.com/advisories/30961
* SECUNIA: 30945
http://secunia.com/advisories/30945
* SECUNIA: 30972
http://secunia.com/advisories/30972

* SECUNIA: 30967
http://secunia.com/advisories/30967
* SECUNIA: 30990
http://secunia.com/advisories/30990
* SECUNIA: 31200
http://secunia.com/advisories/31200
* SECUNIA: 32222
http://secunia.com/advisories/32222
* SECUNIA: 32454
http://secunia.com/advisories/32454
* VUPEN: ADV-2008-2336
http://www.vupen.com/english/advisories/2008/2336
* VUPEN: ADV-2009-1297
http://www.vupen.com/english/advisories/2009/1297

CVE Reference:

CVE-2008-2371 (cve.mitre.org, nvd.nist.gov)

• 18499 PHP memnstr buffer overflow Vulnerability

Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.

This has been reported in versions 4.4.x lower than 4.4.9, and 5.x lower than 5.2.7.

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

References:

* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl
http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded
* CONFIRM:
http://bugs.gentoo.org/show_bug.cgi?id=234102
* CONFIRM:
http://news.php.net/php.cvs/52002
* CONFIRM:
http://www.php.net/archive/2008.php#id2008-08-07-1
* MLIST: [oss-security] 20080808 CVE request: php-5.2.6 overflow issues
http://www.openwall.com/lists/oss-security/2008/08/08/2
* MLIST: [oss-security] 20080808 Re: CVE request: php-5.2.6 overflow issues
http://www.openwall.com/lists/oss-security/2008/08/08/3
* MLIST: [oss-security] 20080808 Re: CVE request: php-5.2.6 overflow issues
http://www.openwall.com/lists/oss-security/2008/08/08/4
* MLIST: [oss-security] 20080813 Re: CVE request: php-5.2.6 overflow issues
http://www.openwall.com/lists/oss-security/2008/08/13/8
* CONFIRM:
http://wiki.rpath.com/Advisories:rPSA-2009-0035
* CONFIRM:
http://support.apple.com/kb/HT3549
* APPLE: APPLE-SA-2009-05-12
http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
* DEBIAN: DSA-1647
http://www.debian.org/security/2008/dsa-1647
* HP: HPSBUX02431
http://marc.info/?l=bugtraq&m=124654546101607&w=2
* MANDRIVA: MDVSA-2009:021
http://www.mandriva.com/security/advisories?name=MDVSA-2009:021
* MANDRIVA: MDVSA-2009:022
http://www.mandriva.com/security/advisories?name=MDVSA-2009:022
* MANDRIVA: MDVSA-2009:023
http://www.mandriva.com/security/advisories?name=MDVSA-2009:023
* MANDRIVA: MDVSA-2009:024
http://www.mandriva.com/security/advisories?name=MDVSA-2009:024
* SUSE: SUSE-SR:2008:018
http://lists.opensuse.org/opensuse-security-announce/2008-09/msg00004.html
* SUSE: SUSE-SR:2008:021

http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00006.html
* CERT: TA09-133A
http://www.us-cert.gov/cas/techalerts/TA09-133A.html
* OSVDB: 47483
http://osvdb.org/47483
* SECTRACK: 1020995
http://www.securitytracker.com/id?1020995
* SECUNIA: 32148
http://secunia.com/advisories/32148
* SECUNIA: 32316
http://secunia.com/advisories/32316
* SECUNIA: 31982
http://secunia.com/advisories/31982
* SECUNIA: 35074
http://secunia.com/advisories/35074
* SECUNIA: 35650
http://secunia.com/advisories/35650
* VUPEN: ADV-2008-2336
http://www.vupen.com/english/advisories/2008/2336
* VUPEN: ADV-2009-1297
http://www.vupen.com/english/advisories/2009/1297
* XF: php-memnstr-bo(44405)
http://xforce.iss.net/xforce/xfdb/44405

CVE Reference:

CVE-2008-3659 (cve.mitre.org, nvd.nist.gov)

- **18500 PHP posix_access directory traversal Vulnerability**

Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attackers to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a local filename after the safe_mode check has successfully run.

This has been reported in versions 5.x lower than 5.2.7.

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

References:

* SREASONRES: 20080617 PHP 5.2.6 posix_access() (posix ext) safe_mode bypass
http://securityreason.com/achievement_securityalert/54
* BUGTRAQ: 20090302 rPSA-2009-0035-1 php php-cgi php-imap php-mcrypt php-mysql php-mysqli php-pgsql php-soap php-xsl php5 php5-cgi php5-imap php5-mcrypt php5-mysql php5-mysqli php5-pear php5-pgsql php5-soap php5-xsl
http://www.securityfocus.com/archive/1/archive/1/501376/100/0/threaded
* CONFIRM:
http://wiki.rpath.com/Advisories:rPSA-2009-0035
* CONFIRM:
http://support.apple.com/kb/HT3549
* APPLE: APPLE-SA-2009-05-12
http://lists.apple.com/archives/security-announce/2009/May/msg00002.html
* HP: HPSBUX02431
http://marc.info/?l=bugtraq&m=124654546101607&w=2
* CERT: TA09-133A
http://www.us-cert.gov/cas/techalerts/TA09-133A.html
* BID: 29797
http://www.securityfocus.com/bid/29797
* SECTRACK: 1020327
http://www.securitytracker.com/id?1020327
* SECUNIA: 35074
http://secunia.com/advisories/35074
* SECUNIA: 35650
http://secunia.com/advisories/35650
* SREASON: 3941
http://securityreason.com/securityalert/3941
* VUPEN: ADV-2009-1297
http://www.vupen.com/english/advisories/2009/1297
* XF: php-posixaccess-security-bypass(43196)
http://xforce.iss.net/xforce/xfdb/43196

CVE Reference:

CVE-2008-2665 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2009-3023 Microsoft CVSS 2.0 Score = 9.0**

Buffer overflow in the FTP server in Microsoft Internet Information Server (IIS) 5.0 and 6.0 allows remote authenticated users to execute arbitrary code via a crafted NLST command that uses wildcards.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2009/2481

BID: http://www.securityfocus.com/bid/36189

MILW0RM: http://www.milw0rm.com/exploits/9559

MILW0RM: http://www.milw0rm.com/exploits/9541

CVE Reference: CVE-2009-3023

- **CVE-2009-3020 Microsoft CVSS 2.0 Score = 7.1**

win32k.sys in Microsoft Windows Server 2003 SP2 allows remote attackers to cause a denial of service (system crash) by referencing a crafted .eot file in the src descriptor of an @font-face Cascading Style Sheets (CSS) rule in an HTML document, possibly related to the Embedded OpenType (EOT) Font Engine, a different vulnerability than CVE-2006-0010, CVE-2009-0231, and CVE-2009-0232. NOTE: some of these details are obtained from third party information.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/52403

BID: http://www.securityfocus.com/bid/36029

OSVDB: http://www.osvdb.org/57016

MILW0RM: http://www.milw0rm.com/exploits/9417

SECUNIA: http://secunia.com/advisories/36250

MISC: http://milw0rm.com/sploits/2009-wwbsod.zip

CVE Reference: CVE-2009-3020

- **CVE-2009-3019 Microsoft CVSS 2.0 Score = 5.0**

Microsoft Internet Explorer 6 on Windows XP SP2 and SP3, and Internet Explorer 7 on Vista, allows remote attackers to cause a denial of service (application crash) via JavaScript code that calls createElement to create an instance of the LI element, and then calls setAttribute to set the value attribute.

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

References:

MILW0RM: http://www.milw0rm.com/exploits/9455

CVE Reference: CVE-2009-3019

- **CVE-2009-3037 Symantec CVSS 2.0 Score = 9.3**

Buffer overflow in xlssr.dll in the Autonomy KeyView XLS viewer (aka File Viewer for Excel), as used in IBM Lotus Notes 5.x through 8.5.x, Symantec Mail Security, Symantec BrightMail Appliance, Symantec Data Loss Prevention (DLP), and other products, allows remote attackers to execute arbitrary code via a crafted .xls spreadsheet attachment.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2009/2389

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg21396492

CONFIRM: http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_adv

BID: http://www.securityfocus.com/bid/36124

BID: http://www.securityfocus.com/bid/36042

SECUNIA: http://secunia.com/advisories/36474

SECUNIA: http://secunia.com/advisories/36472

CVE Reference: CVE-2009-3037

- **CVE-2009-3037 IBM CVSS 2.0 Score = 9.3**

Buffer overflow in xlssr.dll in the Autonomy KeyView XLS viewer (aka File Viewer for Excel), as used in IBM Lotus Notes 5.x through 8.5.x, Symantec Mail Security, Symantec BrightMail Appliance, Symantec Data Loss Prevention (DLP), and other products, allows remote attackers to execute arbitrary code via a crafted .xls spreadsheet attachment.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2009/2389

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg21396492

CONFIRM: http://www.symantec.com/business/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_adv

BID: http://www.securityfocus.com/bid/36124

BID: http://www.securityfocus.com/bid/36042

SECUNIA: http://secunia.com/advisories/36474

SECUNIA: http://secunia.com/advisories/36472

CVE Reference: CVE-2009-3037

- **CVE-2008-7135 ICQ CVSS 2.0 Score = 4.3**

toolbaru.dll in ICQ Toolbar (ICQToolbar) 2.3 allows remote attackers to cause a denial of service (toolbar crash) via a long argument to the IsChecked method, a different vector than CVE-2008-7136.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/41014

BID: http://www.securityfocus.com/bid/28086

MISC: http://www.securiteam.com/exploits/5WP0115NPU.html

CVE Reference: CVE-2008-7135

- **CVE-2008-7136 ICQ CVSS 2.0 Score = 4.3**

toolbaru.dll in ICQ Toolbar (ICQToolbar) 2.3 allows remote attackers to cause a denial of service (toolbar crash) via a long argument to the (1) RequestURL, (2) GetPropertyById, or (3) SetPropertyById method, different vectors than CVE-2008-7135.

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

References:

BID: http://www.securityfocus.com/bid/28118

MISC: http://www.securiteam.com/exploits/5WP0115NPU.html

MILW0RM: http://www.milw0rm.com/exploits/5217

CVE Reference: CVE-2008-7136

- **CVE-2008-7144 RARLAB CVSS 2.0 Score = 10.0**

Multiple unspecified vulnerabilities in RARLAB WinRAR before 3.71 have unknown impact and attack vectors related to crafted (1) ACE, (2) ARJ, (3) BZ2, (4) CAB, (5) GZ, (6) LHA, (7) RAR, (8) TAR, or (9) ZIP files, as demonstrated by the OUSPG PROTOS GENOME test suite for Archive Formats.

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

References:

VUPEN: http://www.vupen.com/english/advisories/2008/0916/references

XF: http://xforce.iss.net/xforce/xfdb/41251

MISC: http://www.ee.oulu.fi/research/ouspg/protos/testing/c10/archive/

MISC: http://www.cert.fi/haavoittuvuudet/joint-advisory-archive-formats.html

SECUNIA: http://secunia.com/advisories/29407

OSVDB: http://osvdb.org/43439

CVE Reference: CVE-2008-7144

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