ScoutNews
The weekly Security update from the makers of SecureScout
November 27, 2009

2009 Issue #48

Table of Contents

Product Focus

Mydoom Worm Scanner - The S4 MyDoom Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by the MyDoom email virus or its variants.

Download Here:
http://www.netvigilance.com/productdownloads?productname=mydoomwormscanner

This Week in Review

iPhone users be aware. Cyber crimes expected on Cyber Monday. The expected Christmas scams and some advice on how to avoid.

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

- **Another iPhone worm, but this one is serious**

Another iPhone worm has been spotted in the wild.

Unlike the previous exploitation, which merely changed a jailbroken iPhone's wallpaper to a picture of Rick Astley of "Rickrolling" fame, this new threat allows hackers to steal sensitive information.

According to security firm Sophos, which wrote about the exploitation after a Dutch ISP spotted it late last week, the worm attacks jailbroken iPhone and iPod Touch devices only. Cnet Security

Full Story :
http://news.cnet.com/8301-13506_3-10403425-17.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Experts expect exploits abound on Cyber Monday**

While Americans gear up for a long holiday weekend, cybercriminals are readying their exploits for Cyber Monday, IT security experts said this week.

"Cyber Monday," the digital equivalent of the brick-and-mortar world's "Black Friday," is one of the busiest online shopping days of the year. It happens Monday, when most employees return to work for the first time since Thanksgiving.

But with the increased propensity to hit the internet for shopping deals comes an augmented security risk. SC Magazine

Full Story :
http://www.scmagazineus.com/experts-expect-exploits-abound-on-cyber-monday/article/158466/?utm_source=feedb

- **McAfee warns about '12 Scams of Christmas'**

Retailers aren't the only ones gearing up for the holiday season. Criminals are also out in force.

To highlight the increased crime during the holidays, security company McAfee has come up with the "12 Scams of Christmas" ranging from bogus electronic greeting cards that deliver malware instead of cheer to fake charities that steal your money and your identity.

It's especially important to be extra careful this time of year, says McAfee's David Marcus. "The bad guys know people are spending more time online, they're paying more bills online so [the criminals] stand a chance of being a bit more successful this time of year. Cnet Security

Full Story :
http://news.cnet.com/8301-19518_3-10403100-238.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Five tips for safe Web shopping**

Web shoppers are a suspicious lot. That's the conclusion of a recent poll conducted by Zogby International and funded by Symantec and the National Cyber Security Alliance. The survey found that 63 percent of online shoppers abandoned a purchase due to security concerns.

Among the reasons given for failing to complete the transaction were sites that asked for too much information, uncertainty about how their personal data would be used by the site, and lack of faith in the site's security. These are all valid concerns.

CNET News reporter Greg Sandoval describes recent Congressional hearings on bogus online loyalty programs that sucker Web shoppers into offers that are loaded with fine print. Sandoval's follow-up report indicates that few of the big-name sites profiting from these programs intend to end their relationships with the companies being scrutinized. Cnet Security

Full Story :
http://news.cnet.com/8301-13880_3-10404891-68.html?part=rss&subj=news&tag=2547-1_3-0-20

- **Big changes in Security Starter Kit 2010**

Black Friday is almost upon us, and the steep hardware discounts mean new computers for many. To help you during these tough economic times, we've refreshed the Download.com Security Starter Kit for 2010. Although nothing can replace common-sense browsing, this collection of freeware security tools will help you protect new machines and old from pernicious threats, large and small. Longtime readers will notice that in addition to changing up our recommended antivirus program, we've fleshed out the Web browsing safety category, and made other changes as well. If you're looking for more than freeware security programs, check out the CNET Download.com Windows Starter Kit for 2010.

In this year's version, you can expect to see Avast chosen ahead of AntiVir as our most favored antivirus app. Despite its odd interface, Avast scored higher than any other freeware antivirus in a third-party test, and it doesn't skimp on protection, either, with e-mail, network, rootkit, and behavioral guards along with its top-rated virus protections. Cnet Security

Full Story :
http://download.cnet.com/8301-2007_4-10405343-12.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

- **13738 MySQL XPath expression employing a scalar expression Denial of Service Vulnerability**

A vulnerability has been reported in MySQL, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when processing XPath expressions containing scalar FilterExp expressions. This can be exploited to crash a vulnerable server by e.g. invoking the "ExtractValue()" or "UpdateXML()"

functions with a specially crafted XPath expression.

Versions affected are 5.1.5 through 5.1.31 inclusive and 6.0.0 through 6.0.9 inclusive. No versions of 5.0, 4.1, 4.0 or 3.n are affected.

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

References:

* CONFIRM:
http://bugs.mysql.com/bug.php?id=42495
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-32.html
* CONFIRM:
http://dev.mysql.com/doc/refman/6.0/en/news-6-0-10.html
* BID: 33972
http://www.securityfocus.com/bid/33972
* SECTRACK: 1021786
http://www.securitytracker.com/id?1021786
* SECUNIA: 34115
http://secunia.com/advisories/34115
* VUPEN: ADV-2009-0594
http://www.vupen.com/english/advisories/2009/0594
* XF: mysql-xpath-dos(49050)
http://xforce.iss.net/xforce/xfdb/49050

CVE Reference:

CVE-2009-0819 (cve.mitre.org, nvd.nist.gov)

• 13739 MySQL "vio_verify_callback()" Man-in-the-Middle Vulnerability

An error exists within the "vio_verify_callback()" function in MySQL clients that are linked against OpenSSL libraries. This can potentially be exploited to conduct MitM (Man-in-the-Middle) attacks e.g. via a MySQL server using a certificate with a depth of zero.

The issue has been fixed in versions 4.1.26, 5.0.88, 5.1.41, 5.5.0, and 6.0.14.

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

References:

* SECUNIA: SA37372
http://secunia.com/advisories/37372/
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html
* CONFIRM:
http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html
* CONFIRM:
http://bugs.mysql.com/47320

CVE Reference:

• 13740 MySQL "SELECT" statements containing sub-queries in the "WHERE" clause Denail of Service Vulnerability

An error is caused due to missing error handling for "SELECT" statements containing sub-queries in the "WHERE" clause, which can be exploited to cause a server to crash.

The issue has been fixed in versions 5.0.88, 5.1.41, 5.5.0, and 6.0.14.

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

References:

* SECUNIA: SA37372
http://secunia.com/advisories/37372/
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html
* CONFIRM:
http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html
* CONFIRM:
http://bugs.mysql.com/bug.php?id=48291

CVE Reference:

• 13741 MySQL "GeomFromWKB()" Denail of Service Vulnerability

The "GeomFromWKB()" function fails to preserve an argument's null-value flag when handling geometry values as the first argument. This can be exploited to cause a server to crash.

The issue has been fixed in versions 5.0.88, 5.1.41, 5.5.0, and 6.0.14.

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

References:

* SECUNIA: SA37372
http://secunia.com/advisories/37372/
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html
* CONFIRM:
http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html
* CONFIRM:
http://bugs.mysql.com/bug.php?id=47780

CVE Reference:

• 18604 Oracle Application Server - Portal component unspecified Vulnerability (oct-2009/CVE-2009-3407)

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

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
* CERT: TA09-294A
http://www.us-cert.gov/cas/techalerts/TA09-294A.html
* BID: 36753
http://www.securityfocus.com/bid/36753
* OSVDB: 59116
http://osvdb.org/59116
* SECTRACK: 1023058
http://www.securitytracker.com/id?1023058
* SECUNIA: 37099
http://secunia.com/advisories/37099

CVE Reference:

CVE-2009-3407 (cve.mitre.org, nvd.nist.gov)

• 18605 Oracle Application Server - Business Intelligence Enterprise Edition component unspecified Vulnerability (oct-2009/CVE-2009-1990)

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Business Intelligence Enterprise Edition" component.

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

References:

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2009.html
* CERT: TA09-294A
http://www.us-cert.gov/cas/techalerts/TA09-294A.html
* BID: 36749
http://www.securityfocus.com/bid/36749
* OSVDB: 59117
http://osvdb.org/59117
* SECTRACK: 1023058
http://www.securitytracker.com/id?1023058
* SECUNIA: 37099
http://secunia.com/advisories/37099

CVE Reference:

CVE-2009-1990 (cve.mitre.org, nvd.nist.gov)

• 18606 PHP issing sanity checks around exif processing Vulnerability

Unspecified vulnerability in PHP 5.2.x and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."

The issue has been fixed in PHP versions 5.3.1.

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

References:

* MLIST: [oss-security] 20091120 CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/2
* MLIST: [oss-security] 20091120 Re: CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/3
* MLIST: [php-announce] 20091119 5.3.1 Release announcement
http://news.php.net/php.announce/79
* CONFIRM:
http://www.php.net/ChangeLog-5.php#5.2.11
* CONFIRM:
http://www.php.net/releases/5_2_11.php
* CONFIRM:
http://support.apple.com/kb/HT3937
* CONFIRM:
http://www.php.net/ChangeLog-5.php
* CONFIRM:
http://www.php.net/releases/5_3_1.php
* APPLE: APPLE-SA-2009-11-09-1
http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html
* OSVDB: 58186
http://www.osvdb.org/58186
* SECTRACK: 1022914
http://www.securitytracker.com/id?1022914
* SECUNIA: 36791
http://secunia.com/advisories/36791
* SECUNIA: 37412
http://secunia.com/advisories/37412
* VUPEN: ADV-2009-3184
http://www.vupen.com/english/advisories/2009/3184
* BID: 36449
http://www.securityfocus.com/bid/36449

CVE Reference:

CVE-2009-3292 (cve.mitre.org, nvd.nist.gov)

• 18607 PHP safe_mode bypass in tempnam() Vulnerability

The tempnam function in ext/standard/file.c in PHP 5.2.11 and earlier, and 5.3.x before 5.3.1, allows context-dependent attackers to bypass safe_mode restrictions, and create files in group-writable or world-writable directories, via the dir and prefix arguments.

The issue has been fixed in PHP versions 5.3.1.

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

References:

* BID: 36449
http://www.securityfocus.com/bid/36449
* MLIST: [oss-security] 20091120 CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/2
* MLIST: [oss-security] 20091120 Re: CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/3
* MLIST: [oss-security] 20091120 Re: CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/5
* MLIST: [php-announce] 20091119 5.3.1 Release announcement
http://news.php.net/php.announce/79
* CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/standard/file.c?view=log
* CONFIRM:

http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/standard/file.c?view=log
* CONFIRM:
http://svn.php.net/viewvc?view=revision&revision=288945
* CONFIRM:
http://www.php.net/ChangeLog-5.php
* CONFIRM:
http://www.php.net/releases/5_3_1.php
* SECUNIA: 37412
http://secunia.com/advisories/37412
* SREASON: 6601
http://securityreason.com/securityalert/6601

CVE Reference:

CVE-2009-3557 (cve.mitre.org, nvd.nist.gov)

• 18608 PHP open_basedir bypass in posix_mkfifo() Vulnerability

The posix_mkfifo function in ext/posix/posix.c in PHP 5.2.11 and earlier, and 5.3.x before 5.3.1, allows context-dependent attackers to bypass open_basedir restrictions, and create FIFO files, via the pathname and mode arguments, as demonstrated by creating a .htaccess file.

The issue has been fixed in PHP versions 5.3.1.

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

References:

* BID: 36449
http://www.securityfocus.com/bid/36449
* MLIST: [oss-security] 20091120 CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/2
* MLIST: [oss-security] 20091120 Re: CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/3
* MLIST: [oss-security] 20091120 Re: CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/5
* MLIST: [php-announce] 20091119 5.3.1 Release announcement
http://news.php.net/php.announce/79
* CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/posix/posix.c?view=log
* CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/posix/posix.c?view=log
* CONFIRM:
http://svn.php.net/viewvc?view=revision&revision=288943
* CONFIRM:
http://www.php.net/ChangeLog-5.php
* CONFIRM:
http://www.php.net/releases/5_3_1.php
* SECUNIA: 37412
http://secunia.com/advisories/37412
* SREASON: 6600
http://securityreason.com/securityalert/6600

CVE Reference:

CVE-2009-3558 (cve.mitre.org, nvd.nist.gov)

• 18609 PHP DOS via temporary file exhaustion Vulnerability

PHP 5.2.11, and 5.3.x before 5.3.1, does not restrict the number of temporary files created when handling a multipart/form-data POST request, which allows remote attackers to cause a denial of service (resource exhaustion), and makes it easier for remote attackers to exploit local file inclusion vulnerabilities, via multiple requests, related to lack of support for the max_file_uploads directive.

The issue has been fixed in PHP versions 5.3.1.

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

References:

* BID: 36449
http://www.securityfocus.com/bid/36449
* FULLDISC: 20091120 PHP "multipart/form-data" denial of service

http://seclists.org/fulldisclosure/2009/Nov/228
* MLIST: [oss-security] 20091120 CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/2
* MLIST: [oss-security] 20091120 Re: CVE request: php 5.3.1 update
http://www.openwall.com/lists/oss-security/2009/11/20/7
* MLIST: [php-announce] 20091119 5.3.1 Release announcement
http://news.php.net/php.announce/79
* CONFIRM:
http://www.php.net/ChangeLog-5.php
* CONFIRM:
http://www.php.net/releases/5_3_1.php

CVE Reference:

CVE-2009-4017 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-4054 Microsoft CVSS 2.0 Score = 10.0

Microsoft Internet Explorer 6 and 7 allows remote attackers to execute arbitrary code via vectors involving a call to the getElementsByTagName method for the STYLE tag name, selection of the single element in the returned list, and a change to the outerHTML property of this element. NOTE: some of these details are obtained from third party information.

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

References:

BID: http://www.securityfocus.com/bid/37085

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/507984/100/0/threaded

CVE Reference: CVE-2009-4054

• CVE-2009-4073 Microsoft CVSS 2.0 Score = 5.0

The printing functionality in Microsoft Internet Explorer 8 allows remote attackers to discover a local pathname, and possibly a local username, by reading the dc:title element of a PDF document that was generated from a local web page.

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

References:

MISC: http://www.theregister.co.uk/2009/11/23/internet_explorer_file_disclosure_bug/

BUGTRAQ: http://www.securityfocus.com/archive/1/archive/1/508010/100/0/threaded

MISC: http://securethoughts.com/2009/11/millions-of-pdf-invisibly-embedded-with-your-internal-disk-paths/

CVE Reference: CVE-2009-4073

• CVE-2009-3843 HP CVSS 2.0 Score = 10.0

HP Operations Manager 8.10 on Windows contains a "hidden account" in the XML file that specifies Tomcat users, which allows remote attackers to conduct unrestricted file upload attacks, and thereby execute arbitrary code, by using the org.apache.catalina.manager.HTMLManagerServlet class to make requests to manager/html/upload.

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

References:

XF: http://xforce.iss.net/xforce/xfdb/54361

MISC: http://www.zerodayinitiative.com/advisories/ZDI-09-085/

OSVDB: http://www.osvdb.org/60317

SECTRACK: http://securitytracker.com/id?1023222

SECUNIA: http://secunia.com/advisories/37444

HP: http://marc.info/?l=bugtraq&m=125873415424980&w=2

HP: http://marc.info/?l=bugtraq&m=125873415424980&w=2

CVE Reference: CVE-2009-3843

- **CVE-2009-4052 IBM CVSS 2.0 Score = 4.3**

Multiple cross-site scripting (XSS) vulnerabilities in the JSF Widget Library Runtime in IBM Rational Application Developer for WebSphere Software before 7.0.0.10 and Rational Software Architect before 7.0.0.10 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) the JSF Tree Control and (2) the JavaScript Resource Servlet.

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

References:

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg27012558

CONFIRM: http://www-01.ibm.com/support/docview.wss?uid=swg27012378

XF: http://xforce.iss.net/xforce/xfdb/54360

BID: http://www.securityfocus.com/bid/37083

OSVDB: http://www.osvdb.org/60319

AIXAPAR: http://www-01.ibm.com/support/docview.wss?uid=swg1PK94324

AIXAPAR: http://www-01.ibm.com/support/docview.wss?uid=swg1PK90616

SECUNIA: http://secunia.com/advisories/37442

CVE Reference: CVE-2009-4052

- **CVE-2009-3558 PHP CVSS 2.0 Score = 7.5**

The posix_mkfifo function in ext/posix/posix.c in PHP 5.2.11 and earlier, and 5.3.x before 5.3.1, allows context-dependent attackers to bypass open_basedir restrictions, and create FIFO files, via the pathname and mode arguments, as demonstrated by creating a .htaccess file.

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

References:

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/5

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/3

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/2

CONFIRM: http://svn.php.net/viewvc?view=revision&revision=288943

CONFIRM: http://www.php.net/releases/5_3_1.php

CONFIRM: http://www.php.net/ChangeLog-5.php

CONFIRM: http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/posix/posix.c?view=log

CONFIRM: http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/posix/posix.c?view=log

SREASON: http://securityreason.com/securityalert/6600

SECUNIA: http://secunia.com/advisories/37412

MLIST: http://news.php.net/php.announce/79

CVE Reference: CVE-2009-3558

- **CVE-2009-3559 PHP CVSS 2.0 Score = 7.5**

** DISPUTED ** main/streams/plain_wrapper.c in PHP 5.3.x before 5.3.1 does not recognize the safe_mode_include_dir directive, which allows context-dependent attackers to have an unknown impact by triggering

the failure of PHP scripts that perform include or require operations, as demonstrated by a script that attempts to perform a require_once on a file in a standard library directory. NOTE: a reliable third party reports that this is not a vulnerability, because it results in a more restrictive security policy.

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

References:

CONFIRM: http://www.php.net/releases/5_3_1.php

CONFIRM: http://www.php.net/ChangeLog-5.php

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/5

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/3

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/2

MLIST: http://news.php.net/php.announce/79

MISC: http://bugs.php.net/bug.php?id=50063

CVE Reference: CVE-2009-3559

- **CVE-2009-3557 PHP CVSS 2.0 Score = 5.0**

The tempnam function in ext/standard/file.c in PHP 5.2.11 and earlier, and 5.3.x before 5.3.1, allows context-dependent attackers to bypass safe_mode restrictions, and create files in group-writable or world-writable directories, via the dir and prefix arguments.

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

References:

CONFIRM: http://www.php.net/releases/5_3_1.php

CONFIRM: http://www.php.net/ChangeLog-5.php

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/5

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/3

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/2

CONFIRM: http://svn.php.net/viewvc?view=revision&revision=288945

CONFIRM: http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/ext/standard/file.c?view=log

CONFIRM: http://svn.php.net/viewvc/php/php-src/branches/PHP_5_2/ext/standard/file.c?view=log

SREASON: http://securityreason.com/securityalert/6601

SECUNIA: http://secunia.com/advisories/37412

MLIST: http://news.php.net/php.announce/79

CVE Reference: CVE-2009-3557

- **CVE-2009-4017 PHP CVSS 2.0 Score = 5.0**

PHP 5.2.11, and 5.3.x before 5.3.1, does not restrict the number of temporary files created when handling a multipart/form-data POST request, which allows remote attackers to cause a denial of service (resource exhaustion), and makes it easier for remote attackers to exploit local file inclusion vulnerabilities, via multiple requests, related to lack of support for the max_file_uploads directive.

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

References:

CONFIRM: http://www.php.net/releases/5_3_1.php

CONFIRM: http://www.php.net/ChangeLog-5.php

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/2

MLIST: http://www.openwall.com/lists/oss-security/2009/11/20/7

FULLDISC: http://seclists.org/fulldisclosure/2009/Nov/228

MLIST: http://news.php.net/php.announce/79

CVE Reference: CVE-2009-4017

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