netVigilance
assurance has arrived

# ScoutNews

*The weekly Security update from the makers of SecureScout*

2008 Issue # 19

May 9, 2008

**Table of Contents**



## Product Focus

**Much anticipated "Negev" released.**

Our Web-interface for the Perimeter Service is now running dynamic pages based on "Ajax", giving a much improved response time and customer experience. Existing customers can log right into the new system from the usual login page.

**Sasser Worm Scanner** – The Sasser Worm 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 Microsoft SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

CTO Jesper Jurcenoks of netVigilance is the keynote speaker at the ITEC Conference & Exhibition 2008 in Dallas June 4-5, see
**http://www.netvigilance.com/events**

## This Week in Review

Safe Oracle still a way to go. An opinion on trust. Hackersafe sites not so safe. Vuln found in software for industrial plants.

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

### ❖ Is your Oracle database really secure?

While Oracle databases are nowhere near as vulnerable as they were five years ago, there is still a great deal of attention being paid to them by both security professionals and hackers alike.

David Litchfield, a renowned Oracle database hacker and author of The Oracle Hacker's Handbook, revealed yesterday at ITWeb Security Summit 2008 only a handful of the various ways in which even the modern Oracle database is vulnerable to attack.

itweb

Full Story :
http://www.itweb.co.za/sections/enterprise/2008/0805081345.asp?S=Security&A=SEC&O=FRGN

### ❖ How Can We Improve Code Signing?

Opinion: An effort to develop standards to make it more effective and meaningful is under way.

I've always been a fan of code signing. It seems clear to me that trust is a major issue for code you bring onto your system, and digital signatures can improve trust.

But it's also clear that code signing is a messed-up process. On popular general-purpose computers it's used widely only on Windows, and nowhere near as widely as it might. Certain aspects of code signing on Windows, especially certificate revocation, are a mess.

eweek

Full Story :
http://www.eweek.com/c/a/Security/How-Can-We-Improve-Code-Signing/

### ❖ XSS vulnerability found in McAfee HackerSafe sites

For the second time this year, a security researcher has found websites certified as McAfee HackerSafe that contain vulnerabilities.

Russ McRee, a security consultant for HolisticInfoSec.org, discovered a number of websites that carry the HackerSafe logo, but have been found to be vulnerable to cross-site scripting (XSS) errors. According to a blog post written by McRee, the vulnerabilities make it possible for hackers to access authentication credentials or send users to malicious websites.

scmagazine

Full Story :

http://www.scmagazineus.com/XSS-vulnerability-found-in-McAfee-HackerSafe-sites/article/109585/?DCMP=EMC-SCUS_Newswire

### ❖ Rare SCADA vulnerability discovered

Researchers have discovered a rare bug in a Windows-based control software package used by as many as one-third of the world's industrial plants.

The vulnerable software component, Wonderware SuiteLink, is used to help facilitate communications over TCP/IP networks for SCADA (supervisory control and data acquisition) systems, according to an advisory from Core Security Technologies, which discovered the flaw.

scmagazine

Full Story :
http://www.scmagazineus.com/Rare-SCADA-vulnerability-discovered/article/109956/

# New Vulnerabilities Tested in SecureScout

- **17780 PHP not protecting against deep recursions**

PHP 4.4.2 and 5.1.2 allows local users to cause a crash (segmentation fault) by defining and executing a recursive function. NOTE: it has been reported by a reliable third party that some later versions are also affected.

The vulnerability has been confirmed in version 4.4.x and 5.x.

There is no fix for the issue.

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

**References:**

* BUGTRAQ: 20060409 function *() php/apache Crash PHP 4.4.2 and 5.1.2
http://www.securityfocus.com/archive/1/archive/1/430453/100/0/threaded
* BUGTRAQ: 20060410 Re: function *() php/apache Crash PHP 4.4.2 and 5.1.2
http://www.securityfocus.com/archive/1/archive/1/430598/100/0/threaded
* BUGTRAQ: 20060412 Re: function *() php/apache Crash PHP 4.4.2 and 5.1.2
http://www.securityfocus.com/archive/1/archive/1/430742/100/0/threaded
* BUGTRAQ: 20060414 Re: Re: function *() php/apache Crash PHP 4.4.2 and 5.1.2
http://www.securityfocus.com/archive/1/archive/1/431018/100/0/threaded
* SREASONRES: 20060408 function *() php/apache Crash PHP 4.4.2 and 5.1.2
http://securityreason.com/achievement_securityalert/35
* MISC:
http://www.php-security.org/MOPB/MOPB-02-2007.html
* FRSIRT: ADV-2006-1290
http://www.frsirt.com/english/advisories/2006/1290
* OSVDB: 24485

http://www.osvdb.org/24485
* SECTRACK: 1015880
http://securitytracker.com/id?1015880
* SREASON: 2312
http://securityreason.com/securityalert/2312
* SREASON: 676
http://securityreason.com/securityalert/676
* XF: php-function-dos(25704)
http://xforce.iss.net/xforce/xfdb/25704

**CVE Reference:**

CVE-2006-1549 (cve.mitre.org, nvd.nist.gov)

- **17781 PHP glob() function, bypass open_basedir restrictions**

PHP could allow a remote attacker to bypass security restrictions, caused by a regression error related to the glob() function. An attacker could exploit this vulnerability to bypass open_basedir directives and gain unauthorized access to the system.

The vulnerability has been confirmed in version 4.x lower than 4.4.8.

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

**References:**

* CONFIRM:
http://bugs.php.net/bug.php?id=41655
* CONFIRM:
http://www.php.net/ChangeLog-4.php
* CONFIRM:
http://www.php.net/releases/4_4_8.php
* SLACKWARE: SSA:2008-045-03
http://slackware.com/security/viewer.php?l=slackware-security&y=2008&m=slackware-security.335136
* SECUNIA: 28318
http://secunia.com/advisories/28318
* SECUNIA: 28936
http://secunia.com/advisories/28936
* XF: php-glob-openbasedir-security-bypass(39401)
http://xforce.iss.net/xforce/xfdb/39401

**CVE Reference:**

CVE-2008-0145 (cve.mitre.org, nvd.nist.gov)

- **17782 PHP stack buffer overflow in FastCGI SAPI**

Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.

The vulnerability has been confirmed in version 5.x lower than 5.2.6.

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

**References:**

* CONFIRM:
http://www.php.net/ChangeLog-5.php
* CONFIRM:
http://cvs.php.net/viewvc.cgi/php-src/sapi/cgi/fastcgi.c?r1=1.44&r2=1.45&diff_format=u
* MLIST: [oss-security] 20080502 CVE Request (PHP)
http://www.openwall.com/lists/oss-security/2008/05/02/2
* BID: 29009
http://www.securityfocus.com/bid/29009
* FRSIRT: ADV-2008-1412
http://www.frsirt.com/english/advisories/2008/1412
* SECUNIA: 30048
http://secunia.com/advisories/30048

**CVE Reference:**

CVE-2008-2050 (cve.mitre.org, nvd.nist.gov)

- **17783 PHP incomplete multibyte chars inside escapeshellcmd()**

The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."

The vulnerability has been confirmed in version 5.x lower than 5.2.6.

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

**References:**

* CONFIRM:
http://www.php.net/ChangeLog-5.php
* MLIST: [oss-security] 20080502 CVE Request (PHP)
http://www.openwall.com/lists/oss-security/2008/05/02/2
* BID: 29009
http://www.securityfocus.com/bid/29009
* FRSIRT: ADV-2008-1412
http://www.frsirt.com/english/advisories/2008/1412
* SECUNIA: 30048
http://secunia.com/advisories/30048

**CVE Reference:**

CVE-2008-2051 (cve.mitre.org, nvd.nist.gov)

- **17784 PHP cgi_main.c, incorrect length of PATH_TRANSLATE calculation**

cgi_main.c in PHP before 5.2.6 does not properly calculate the length of PATH_TRANSLATED, which has unknown impact and attack vectors.

The vulnerability has been confirmed in version 5.x lower than 5.2.6.

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

**References:**

* CONFIRM:
http://www.php.net/ChangeLog-5.php
* MLIST: [oss-security] 20080502 CVE Request (PHP)
http://www.openwall.com/lists/oss-security/2008/05/02/2
* BID: 29009
http://www.securityfocus.com/bid/29009
* FRSIRT: ADV-2008-1412
http://www.frsirt.com/english/advisories/2008/1412
* SECUNIA: 30048
http://secunia.com/advisories/30048
* CONFIRM:
http://cvs.php.net/viewvc.cgi/php-src/sapi/cgi/cgi_main.c?r1=1.267.2.15.2.50.2.12&r2=1.267.2.15.2.50.2.13&diff_format=u
* SECTRACK: 1019958
http://www.securitytracker.com/id?1019958
* XF: php-vector-unspecified(42137)
http://xforce.iss.net/xforce/xfdb/42137

**CVE Reference:**

CVE-2008-0599 (cve.mitre.org, nvd.nist.gov)

- **17785 PHP safe_mode bypass in cURL**

curl/interface.c in the cURL library (aka libcurl) in PHP 5.2.4 and 5.2.5 allows context-dependent attackers to bypass safe_mode and open_basedir restrictions and read arbitrary files via a file:// request containing a \x00 sequence.

The vulnerability has been confirmed in version 5.2.4 and 5.2.5.

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

**References:**

* SREASONRES: 20080122 PHP 5.2.5 cURL safe_mode bypass
http://securityreason.com/achievement_securityalert/51
* BUGTRAQ: 20080122 PHP 5.2.5 cURL safe_mode bypass
http://www.securityfocus.com/archive/1/archive/1/486856/100/0/threaded
* FULLDISC: 20080122 PHP 5.2.5 cURL safe_mode bypass

http://lists.grok.org.uk/pipermail/full-disclosure/2008-January/059849.html
* CONFIRM:
http://cvs.php.net/viewcvs.cgi/php-src/NEWS?revision=1.2027.2.547.2.1047&view=markup
* BID: 27413
http://www.securityfocus.com/bid/27413
* SREASON: 3562
http://securityreason.com/securityalert/3562
* XF: php-curlinit-security-bypass(39852)
http://xforce.iss.net/xforce/xfdb/39852

**CVE Reference:**

CVE-2007-4850 (cve.mitre.org, nvd.nist.gov)

- **17786 PHP PCRE Character Class Buffer Overflow**

Buffer overflow in PCRE before 7.6 allows remote attackers to execute arbitrary code via a regular expression containing a character class with a large number of characters with Unicode code points greater than 255.

The vulnerability has been confirmed in PHP version 5.x before 5.2.6.

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

**References:**

* BUGTRAQ: 20080228 rPSA-2008-0086-1 pcre
http://www.securityfocus.com/archive/1/archive/1/488927/100/0/threaded
* CONFIRM:
http://pcre.org/changelog.txt
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=431660
* CONFIRM:
http://ftp.gnome.org/pub/gnome/sources/glib/2.14/glib-2.14.6.news
* CONFIRM:
http://wiki.rpath.com/wiki/Advisories:rPSA-2008-0086
* CONFIRM:
https://issues.rpath.com/browse/RPL-2223
* CONFIRM:
http://wiki.rpath.com/Advisories:rPSA-2008-0086
* DEBIAN: DSA-1499
http://www.debian.org/security/2008/dsa-1499
* FEDORA: FEDORA-2008-1533
https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00371.html
* FEDORA: FEDORA-2008-1783
https://www.redhat.com/archives/fedora-package-announce/2008-February/msg00632.html
* FEDORA: FEDORA-2008-1842
https://www.redhat.com/archives/fedora-package-announce/2008-March/msg00181.html
* GENTOO: GLSA-200803-24

http://security.gentoo.org/glsa/glsa-200803-24.xml
* MANDRIVA: MDVSA-2008:053
http://www.mandriva.com/security/advisories?name=MDVSA-2008:053
* SUSE: SUSE-SR:2008:004
http://lists.opensuse.org/opensuse-security-announce/2008-02/msg00008.html
* UBUNTU: USN-581-1
http://www.ubuntulinux.org/support/documentation/usn/usn-581-1
* BID: 27786
http://www.securityfocus.com/bid/27786
* FRSIRT: ADV-2008-0570
http://www.frsirt.com/english/advisories/2008/0570
* FRSIRT: ADV-2008-0592
http://www.frsirt.com/english/advisories/2008/0592
* SECUNIA: 28923
http://secunia.com/advisories/28923
* SECUNIA: 28960
http://secunia.com/advisories/28960
* SECUNIA: 28985
http://secunia.com/advisories/28985
* SECUNIA: 28996
http://secunia.com/advisories/28996
* SECUNIA: 28957
http://secunia.com/advisories/28957
* SECUNIA: 29027
http://secunia.com/advisories/29027
* SECUNIA: 29048
http://secunia.com/advisories/29048
* SECUNIA: 29175
http://secunia.com/advisories/29175
* SECUNIA: 29267
http://secunia.com/advisories/29267
* SECUNIA: 29282
http://secunia.com/advisories/29282
* XF: pcre-characterclass-bo(40505)
http://xforce.iss.net/xforce/xfdb/40505

**CVE Reference:**

CVE-2008-0674 (cve.mitre.org, nvd.nist.gov)

- **17787 PHP SOAP Extension HTTP Authentication Weak Nonce**

The soap extension in PHP calls php_rand_r with an uninitialized seed variable, which has unknown impact and attack vectors.

The vulnerability has been confirmed in PHP version 4.4.x lower than 4.4.7 and 5.x before 5.2.2.

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

**References:**

* MISC:
http://blog.php-security.org/archives/80-Watching-the-PHP-CVS.html
* MANDRIVA: MDKSA-2007:187
http://www.mandriva.com/security/advisories?name=MDKSA-2007:187
* SUSE: SUSE-SR:2007:015
http://www.novell.com/linux/security/advisories/2007_15_sr.html
* UBUNTU: USN-485-1
http://www.ubuntu.com/usn/usn-485-1
* FRSIRT: ADV-2007-1839
http://www.frsirt.com/english/advisories/2007/1839
* SECUNIA: 25306
http://secunia.com/advisories/25306
* SECUNIA: 26102
http://secunia.com/advisories/26102
* SECUNIA: 26895
http://secunia.com/advisories/26895

**CVE Reference:**

CVE-2007-2728 (cve.mitre.org, nvd.nist.gov)

- **17788 PHP crypt() Race Condition Vulnerability**

PHP 4.x and 5.x before 5.2.1, when running on multi-threaded systems, does not ensure thread safety for libc crypt function calls using protection schemes such as a mutex, which creates race conditions that allow remote attackers to overwrite internal program memory and gain system access.

The vulnerability has been confirmed in PHP version 4.4.x lower than 4.4.8 and 5.x before 5.2.1.

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

**References:**

* MISC:
http://blog.php-security.org/archives/82-Suhosin-0.9.20-and-crypt-Thread-Safety-Vulnerability.html
* BID: 24109
http://www.securityfocus.com/bid/24109
* SECUNIA: 25434
http://secunia.com/advisories/25434
* XF: php-crypt-authentication-bypass(34601)
http://xforce.iss.net/xforce/xfdb/34601

**CVE Reference:**

CVE-2007-2844 (cve.mitre.org, nvd.nist.gov)

- **17789 PHP COM Objects Security Bypass**

The Component Object Model (COM) functions in PHP 5.x on Windows do not follow safe_mode and disable_functions restrictions, which allows context-dependent attackers to bypass intended limitations, as demonstrated by executing objects with the kill bit set in the corresponding ActiveX control Compatibility Flags, executing programs via a function in compatUI.dll, invoking wscript.shell via wscript.exe, invoking Scripting.FileSystemObject via wshom.ocx, and adding users via a function in shgina.dll, related to the com_load_typelib function.

The vulnerability has been confirmed in PHP version 5.x before 5.2.5.

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

**References:**

* MILW0RM: 4553
http://www.milw0rm.com/exploits/4553
* FRSIRT: ADV-2007-3590
http://www.frsirt.com/english/advisories/2007/3590
* SECUNIA: 27280
http://secunia.com/advisories/27280
* XF: php-com-security-bypass(37368)
http://xforce.iss.net/xforce/xfdb/37368

**CVE Reference:**

CVE-2007-5653 (cve.mitre.org, nvd.nist.gov)

# New Vulnerabilities found this Week

### PHP Multiple Vulnerabilities

"Denial of Service"

Some vulnerabilities have been reported in PHP, where some have unknown impacts and others can be exploited by malicious users to bypass certain security restrictions, and potentially by malicious people to cause a DoS (Denial of Service) or to compromise a vulnerable system.

1) An unspecified error in the FastCGI SAPI can be exploited to cause a stack-based buffer overflow.

2) An error in the processing of multibyte characters within the "escapeshellcmd()" and "escapeshellarg()" functions can be exploited to escape the inserted backslash or quote characters via certain multibyte characters.

Successful exploitation allows to bypass the "safe_mode_exec_dir" and "disable_functions" directives, and potentially to inject arbitrary shell commands via user controlled input, but requires that the shell uses a locale with a variable width character (e.g. GBK, EUC-KR, SJIS).

3) A vulnerability is caused due to an error during path translation in cgi_main.c. This can potentially be exploited to execute arbitrary code, but depends on how a targeted application is using PHP.

4) An error in cURL can be exploited to bypass the "safe_mode" directive.

5) A boundary error in PCRE can potentially be exploited by malicious people to cause a DoS or compromise a vulnerable system.

The vulnerabilities are reported in versions prior to 5.2.6.

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

### Akamai Download Manager Code Execution Vulnerability

"Download and execute malicious programs"

A vulnerability has been reported in Akamai Download Manager, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to certain undocumented object parameters, which can be exploited to e.g. download and execute malicious programs when a user is tricked into visiting a malicious site.

The vulnerability is reported in both the ActiveX and Java versions prior to 2.2.3.5.

References:
http://lists.grok.org.uk/pipermail/full-disclosure/2008-April/061923.html

### Novell GroupWise WebAccess Script Insertion

"Script insertion attacks"

Juan Pablo Lopez Yacubian has reported a vulnerability in Novell GroupWise, which can be exploited by malicious people to conduct script insertion attacks.

Input passed via e.g. a .JPG attachment in Novell GroupWise WebAccess is not properly sanitised before being returned to a user. This can be exploited to insert arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site when a malicious .JPG attachment is viewed.

The vulnerability is reported in version 7. Other versions may also be affected.

References:
http://archives.neohapsis.com/archives/bugtraq/2008-04/0330.html

### Bugzilla Security Bypass and Cross-Site Scripting Vulnerabilities

""

Some vulnerabilities have been reported in Bugzilla, which can be exploited by malicious users to bypass certain security restrictions or by malicious people to conduct cross-site scripting attacks.

1) Input passed to certain unspecified parameters is not properly sanitized before being returned to a user when using "Format for Printing" or "Long Format" of a bug list. This can

be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerability is reported in version 2.17.2 and later.

2) It is possible for users without the "canconfirm" privileges to put bugs in the "NEW" or "ASSIGNED" state via the XML-RPC interface.

The vulnerability is reported in version 3.1.3.

An issue that allows spoofing of the reporter of the bug when using email_in.pl has also been reported.

References:
http://www.bugzilla.org/security/2.20.5/

**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