netVigilance
assurance has arrived

# ScoutNews

*The weekly Security update from the makers of SecureScout*

2007 Issue # 11

March 16, 2007

**Table of Contents**



## Product Focus

**Nimda Worm Scanner** – The Nimda 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 MS IE Mime Header Flaw (MS01-020) or have been infected by the Nimda Worm.

## This Week in Review

Cebit talk about internet Interpol. UK financial businesses pays big penalties for missing security. New flaw in IE7 on the wild. US Anti Spy Act legislation considered for the 3rd time.

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

- **Cebit 07: Vista security 'will not last a year'**

We need web Interpol to hit criminals as well as anti-malware says Kasperskhy
Clive Akass at Cebit, Personal Computer World 15 Mar 2007
Windows Vista will be as vulnerable to rogue code as XP within a year, the co-founder of anti-virus firm Kaspersky predicted at Cebit today.

Eugene Kaspersky also called for an “Interpol of the Internet” to counter a new breed

of international high-tech criminals.

His virus analyst Magnus Kalyuki told a press conference that the German equivalent of the FBI had warned of an increase in industrial espionage by Chinese hackers, which had cost on state alone €1bn.

Attacks targeting single companies in this way were particularly hard to tackle because they did not tend to be amenable to generic defences.

Personal ComputerWorld

Full Story :
http://www.pcw.co.uk/personal-computer-world/news/2185632/cebit-07-vista-security

### ❖ High price of failing to tighten IT security

UK financial services businesses should be examining their information security procedures carefully following Nationwide Building Society being slapped with a hefty fine for inadequate data security.

The Financial Services Authority (FSA) imposed a penalty of just under £1m on Nationwide last month for failure to take "reasonable care" to organise its systems to effectively manage information security.

The decision related to the theft of a laptop from a Nationwide employee's home. The computer contained details of about 11 million account holders, and although Pin codes and passwords were not included, the FSA ruled that customers were still exposed to an unacceptable risk.

Computerweekly.com

Full Story :
http://www.computerweekly.com/Articles/2007/03/16/222461/high-price-of-failing-to-tighten-it-security.htm

### ❖ Phishing risk seen in new IE 7 security flaw

Attackers could exploit a new flaw in Internet Explorer 7 (IE 7) to launch phishing expeditions, warns Israeli vulnerability researcher Aviv Raff.

Microsoft said it is investigating the findings of Raff .....who said IE 7 running on Windows XP and Vista is susceptible to cross-site scripting attacks. That combined with a design flaw in the browser could allow digital miscreants to launch phishing schemes against users, he added.

"I think it is a serious vulnerability, because it allows a phisher to take advantage of the user without the need to create a look alike URL," Raff said in an instant message exchange. "The user will see the trusted URL in the address bar and the fake content provided by the phisher."

Raff said he is unaware of any exploits in the wild. Microsoft issued a statement saying that it's investigating the flaw but has seen no evidence of active exploits to date.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2007/03/16/222463/phishing-risk-seen-in-new-ie-7-security-flaw.htm

- **US caution over spyware ban**

Members of a committee of the US Congress have heard a chorus of support for a proposed spyware ban. But that support was tempered by calls for caution by some who fear the bill, without some modifications, could harm internet advertisers.
The Securely Protect Yourself Against Cyber Trespass Act (Spy Act), is sponsored by Rep. Edolphus Towns and would make it unlawful to install software that gathers information, monitors usage, serves up advertisements or modifies browser and other settings on a computer without explicit user consent.

Violations would be treated as unfair or deceptive trade practices subject to enforcement action by the US Federal Trade Commission. The bill also allows fines of up to $3 million for some types of violations.

The Spy Act marks the third time in recent years that the House has considered such legislation. The first time, a similar bill proposed by Rep. Mary Bono passed the House with broad bipartisan support but failed to make it through the Senate. A second attempt by Bono in the last Congress also passed the House with overwhelming support but met with the same fate in the Senate.

TechWorld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=8290&pagtype=samechan

# New Vulnerabilities Tested in SecureScout

- **13525 MySQL Single-Row Subselect Denial of Service**

S. Streichbier and B. Mueller have reported a vulnerability in MySQL, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL-pointer dereference error within the filesort() function when processing certain single-row subselect queries sorted using the "ORDER BY" clause. This can be exploited to crash the service via a specially crafted SQL query.

The vulnerability has been reported in version prior to 5.0.37.

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

**References:**

Original advisory:
http://www.sec-consult.com/284.html

Other references:
* BUGTRAQ:20070309 SEC Consult SA-20070309-0 :: MySQL 5 Single Row Subselect Denial of Service
* URL:http://www.securityfocus.com/archive/1/archive/1/462339/100/0/threaded
* BID:22900
* URL:http://www.securityfocus.com/bid/22900

**CVE Reference:** CVE-2007-1420

### ❖ 16460 Internet Explorer 7 navcancl.htm Cross-Site Scripting Vulnerability (Remote File Checking)

Aviv Raff has discovered a vulnerability in Internet Explorer 7, which can be exploited by malicious people to conduct phishing attacks.

An input validation error exists in the local resource page "navcancl.htm" when generating the "Refresh the page" link. This can be exploited to inject arbitrary script code to e.g. spoof the contents of an arbitrary site when the user clicks on the "Refresh the page" link.

The vulnerability is confirmed in Internet Explorer 7 on a fully patched Windows XP SP2 system. Other versions may also be affected.

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

**References:**

Original advisory:
http://aviv.raffon.net/2007/03/14/PhishingUsingIE7LocalResourceVulnerability.aspx

Other references:
http://secunia.com/advisories/24535/

**CVE Reference:**

### ❖ 16461 Linux Kernel NULL Pointer Dereferences Vulnerability

A vulnerability has been reported in the Linux Kernel, which potentially can be exploited by malicious people to cause a DoS (Denial of Service).

NULL pointer dereferences within net/netfilter/nfnetlink_log.c can potentially be exploited to cause a kernel panic by sending specially crafted packets to a vulnerable system.

The vulnerability is reported in version prior to 2.6.20.3

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

**References:**

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.3

Other references:
http://secunia.com/advisories/24492/

Product Homepage:
http://kernel.org/

**CVE Reference:**

### ❖ 16462 Linux Kernel assembling fragmented IPv6 packets, bypass rulesets Vulnerability

A vulnerability has been reported in the Linux Kernel, which potentially can be exploited by malicious people to bypass security restrictions.

An error exists within conntrack when assembling fragmented IPv6 packets. This can potentially be exploited to bypass certain rulesets that accept ESTABLISHED packets early.

The vulnerability is reported in version prior to 2.6.20.3

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

**References:**

Original advisory:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.3

Other references:
http://secunia.com/advisories/24492/

Product Homepage:
http://kernel.org/

**CVE Reference:**

### ❖ 16463 Linux Kernel "ipv6_getsockopt_sticky()" DoS and Information Leak Vulnerability

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or disclose potentially sensitive information.

The vulnerability is due to a NULL pointer dereference within the "ipv6_getsockopt_sticky()" function in net/ipv6/ipv6_sockglue.c. This can be exploited to crash the kernel or disclose kernel memory.

The vulnerability is reported in versions prior to 2.6.20.2.

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

**References:**

Original advisory:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.2
http://bugzilla.kernel.org/show_bug.cgi?id=8134

Other references:
http://www.kb.cert.org/vuls/id/920689

Product Homepage:
http://kernel.org/

**CVE Reference:** CVE-2007-1000

### ❖ 17268 PHP "session_regenerate_id()" double free error, arbitrary code execution Vulnerability

Stefan Esser has reported a vulnerability in PHP, which can be exploited by malicious users to compromise a vulnerable system.

A double free error within the "session_regenerate_id()" function can be exploited to execute arbitrary code with the privileges of the PHP interpreter.

The vulnerability is reported in version 5.2.0 and 5.2.1. Other versions may also be affected.

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

**References:**

Original advisory:
http://www.php-security.org/MOPB/MOPB-22-2007.html

Other references:
http://secunia.com/advisories/24505/

**CVE Reference:**

### ❖ 17309 PHP double free error within the handling of rejected sessions, arbitrary code execution Vulnerability

Stefan Esser has reported a vulnerability in PHP, which can be exploited by malicious users to compromise a vulnerable system.

A double free error within the handling of rejected sessions in PHP's internal storage module can be exploited to execute arbitrary code with the privileges of the PHP interpreter.

Successful exploitation requires that a user can e.g. upload and execute malicious PHP scripts. Remote exploitation may be possible, but has not currently been proven.

The vulnerability is reported in version 5.2.0 and 5.2.1. Other versions may also be affected.

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

**References:**

Original advisory:
http://www.php-security.org/MOPB/MOPB-22-2007.html

Other references:
http://secunia.com/advisories/24505/

**CVE Reference:**

### ❖ 17347 PHP "snmpget()" Buffer Overflow Vulnerability

rgod has reported a vulnerability in PHP4, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to a boundary error in the "snmpget()" function. This can be exploited to cause a stack-based buffer overflow via an overly long argument and execute arbitrary code, bypassing security restrictions like the "disable_functions" directive.

The vulnerability is reported in version 4.4.6. Other versions may also be affected.

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

**References:**

Original advisory:
http://milw0rm.com/exploits/3439

Other references:
* BID:22893
* URL:http://www.securityfocus.com/bid/22893

**CVE Reference:** CVE-2007-1413

### ❖ 17941 w-agora Multiple Path Disclosure Vulnerabilities

w-agora is a set of scripts written in PHP intended to allow users to share, exchange and publish information, files and discussions over the web.

Security issues in the product allow attackers to gather the true path of the server-side scripts.

This vulnerabilities can be exploited only when PHP register_globals is On.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Gather info** Risk: **Low**

**References:**

Original Advisory:
http://netvigilance.com/advisory0014

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0606
http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-0606

Product Home-Page:
http://www.w-agora.net/

**CVE Reference:** CVE-2007-0606

### ❖ 17942 w-agora Information Disclosure Vulnerability

w-agora is a set of scripts written in PHP intended to allow users to share, exchange and publish information, files and discussions over the web.

A security issue in the product allows attackers to disclose the contents of the globals.inc file and see the true server paths to the main scripts.

This vulnerabilities can be exploited only when PHP register_globals is On.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Gather info** Risk: **Low**

**References:**

Original Advisory:
http://netvigilance.com/advisory0015

Other references:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0607

http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-0607

Product Home-Page:
http://www.w-agora.net/

**CVE Reference:** CVE-2007-0607

# New Vulnerabilities found this Week

**Internet Explorer 7 navcancl.htm Cross-Site Scripting Vulnerability**
"Phishing attacks"

Aviv Raff has discovered a vulnerability in Internet Explorer 7, which can be exploited by malicious people to conduct phishing attacks.

An input validation error exists in the local resource page "navcancl.htm" when generating the "Refresh the page" link. This can be exploited to inject arbitrary script code to e.g. spoof the contents of an arbitrary site when the user clicks on the "Refresh the page" link.

The vulnerability is confirmed in Internet Explorer 7 on a fully patched Windows XP SP2 system. Other versions may also be affected.

References:
http://aviv.raffon.net/2007/03/14/PhishingUsingIE7LocalResourceVulnerability.aspx
http://descriptions.securescout.com/tc/16460

**PHP Session Handling Double Free Vulnerabilities**
"Execute arbitrary code"

Stefan Esser has reported some vulnerabilities in PHP, which can be exploited by malicious users to compromise a vulnerable system.

1) A double free error within the "session_regenerate_id()" function can be exploited to execute arbitrary code with the privileges of the PHP interpreter.

2) A double free error within the handling of rejected sessions in PHP's internal storage module can be exploited to execute arbitrary code with the privileges of the PHP interpreter.

Successful exploitation requires that a user can e.g. upload and execute malicious PHP scripts. Remote exploitation may be possible, but has not currently been proven.

The vulnerabilities are reported in version 5.2.0 and 5.2.1. Other versions may also be affected.

References:
http://www.php-security.org/MOPB/MOPB-22-2007.html
http://descriptions.securescout.com/tc/17268
http://descriptions.securescout.com/tc/17309

**Linux Kernel NULL Pointer Dereferences and Security Bypass**
"Denial of Service"

Some vulnerabilities have been reported in the Linux Kernel, which potentially can be exploited by malicious people to bypass certain security restrictions or cause a DoS (Denial of Service).

1) NULL pointer dereferences within net/netfilter/nfnetlink_log.c can potentially be exploited to cause a kernel panic by sending specially crafted packets to a vulnerable system.

2) An error exists within conntrack when assembling fragmented IPv6 packets. This can potentially be exploited to bypass certain rulesets that accept ESTABLISHED packets early.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.3
http://descriptions.securescout.com/tc/16461
http://descriptions.securescout.com/tc/16462

**Linux Kernel "ipv6_getsockopt_sticky()" DoS and Information Leak**
"Denial of Service; Information disclosure"

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or disclose potentially sensitive information.

The vulnerability is due to a NULL pointer dereference within the "ipv6_getsockopt_sticky()" function in net/ipv6/ipv6_sockglue.c. This can be exploited to crash the kernel or disclose kernel memory.

The vulnerability is reported in versions prior to 2.6.20.2.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.2
http://descriptions.securescout.com/tc/16463

**MySQL Single-Row Subselect Denial of Service**
"Denial of Service"

S. Streichbier and B. Mueller have reported a vulnerability in MySQL, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL-pointer dereference error within the filesort() function when processing certain single-row subselect queries sorted using the "ORDER BY" clause. This can be exploited to crash the service via a specially crafted SQL query.

References:
http://www.sec-consult.com/284.html
http://descriptions.securescout.com/tc/13525

**PHP "snmpget()" Buffer Overflow Vulnerability**
"Execute arbitrary code"

rgod has reported a vulnerability in PHP4, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to a boundary error in the "snmpget()" function. This can be exploited to cause a stack-based buffer overflow via an overly long argument and execute arbitrary code, bypassing security restrictions like the "disable_functions" directive.

The vulnerability is reported in version 4.4.6. Other versions may also be affected.

References:
http://milw0rm.com/exploits/3439
http://descriptions.securescout.com/tc/17347

**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