netVigilance
assurance has arrived

# ScoutNews

*The weekly Security update from the makers of SecureScout*

2008 Issue # 21

May 23, 2008

**Table of Contents**



## Product Focus

**Task Scheduler Vulnerability Scanner** – The 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).

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

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

- **PCI: a matter of timing**

PCI is a subject on which reams have been written already, but in my recent work I have seen it in a different light. For all the technical advice given - and to a large extent practiced - the one thing a project manager should be most aware of seems

to be the thing that is most overlooked: timing. I will even stick my neck out and say that it has been the difference between success and failure in every project I have been involved with.
Visa and MasterCard have so far focused most of their attention on the tier-one merchants - firms that process more than six million transactions a year. This seemingly arbitrary tiering basically represents the point on the curve where the card companies have a "manageable" number of retailers to police - and now that policing operation is under way. Although there is no publicly available information about companies being fined in the UK, a large information processor was recently threatened with having its transaction-processing rights removed after a significant breach was made public.

computerweekly

Full Story :
http://www.computerweekly.com/Articles/2008/05/22/230777/pci-a-matter-of-timing.htm

### ❖ "Silent Love China" Launches Massive Web Attack

A new attack has been detected on the Internet, no less than 9,000 websites being already affected by an exploit codenamed "Silent Love China". SiliconRepublic.com writes that the infection attempts to inject some sort of malicious code into popular websites and steal usernames and passwords belonging to visitors. Similar iFrame attacks were spotted in the past but this time, hackers are especially focused on stealing users' information and not on harming the website, Damian Saunders, Citrix official, told the source mentioned above.
"The virus doesn't threaten the owner of the site, it threatens the user. What happens with this type of attack is rather than destroy a website, the hacker plants a code using SQL injection," explains Damian Saunders, manager of Citrix's applications networking group.

softpedia

Full Story :
http://news.softpedia.com/news/Silent-Love-China-Launches-Massive-Web-Attack-86125.shtml

### ❖ Feds encrypt 800,000 laptops; 1.2 million to go

Encryption software sales boom against backdrop of more stolen laptop cases
U.S. government agencies are scrambling to plug one of their biggest security holes: sensitive information -- names, addresses and Social Security numbers, for example -- stored on laptops, handhelds and thumb drives.
In the last year, agencies have purchased 800,000 licenses for encryption software through the federal Data at Rest (DAR) Encryption program, which is run jointly by the General Services Administration and the U.S. Department of Defense.

networkworld

Full Story :
http://www.networkworld.com/news/2008/052008fedlaptops.html?fsrc=netflash-rss

### ❖ Countering cyber terrorism in third-world countries

Threats to cyberspace can launch from anywhere in the world. And their effect can be especially devastating to emerging economies in third-world countries.

To help counter such threats, the SANS Institute of Bethesda, Md., committed $1 million in time and services for a joint project with the International Multilateral Partnership Against Cyber-Terrorism (IMPACT) to increase the cyberdefense capacity of developing countries.The donation, announced at the World Cyber Security Summit (WCSS) in Kuala Lumpur, Malaysia, will help provide high-quality security for national cyberinfrastructure and government websites. Instructors will be trained so that member governments can maintain high-capacity cyberdefenses.

scmagazine

Full Story :
http://www.scmagazineus.com/Countering-cyber-terrorism-in-third-world-countries/article/110477/

# New Vulnerabilities Tested in SecureScout

### • 13640 MySQL yaSSL Denial of Service Vulnerability

yaSSL 1.7.5 and earlier, as used in MySQL and possibly other products, allows remote attackers to cause a denial of service (crash) via a Hello packet containing a large size value, which triggers a buffer over-read in the HASHwithTransform::Update function in hash.cpp.

The security issue has been reported in versions:
MySQL 5.0.x before 5.0.58, 5.1.x before 5.1.24, and 6.0.x before 6.0.5

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

**References:**

* BUGTRAQ: 20080104 Multiple vulnerabilities in yaSSL 1.7.5
http://www.securityfocus.com/archive/1/archive/1/485810/100/0/threaded
* CONFIRM:
http://bugs.mysql.com/33814
* CONFIRM:
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html
* DEBIAN: DSA-1478
http://www.debian.org/security/2008/dsa-1478
* UBUNTU: USN-588-1
http://www.ubuntu.com/usn/usn-588-1
* BID: 27140
http://www.securityfocus.com/bid/27140
* FRSIRT: ADV-2008-0560
http://www.frsirt.com/english/advisories/2008/0560/references

* SECUNIA: 28324
http://secunia.com/advisories/28324
* SECUNIA: 28597
http://secunia.com/advisories/28597
* SECUNIA: 29443
http://secunia.com/advisories/29443
* SREASON: 3531
http://securityreason.com/securityalert/3531

**CVE Reference:**

CVE-2008-0227 (cve.mitre.org, nvd.nist.gov)

- **16926 Mozilla Firefox _cairo_pen_init Heap based buffer overflow Vulnerability (Remote File Checking)**

Heap-based buffer overflow in the _cairo_pen_init function in Mozilla Firefox, allows remote attackers to execute arbitrary code via a large stroke-width attribute in the clipPath element in an SVG file.

The vulnerability is confirmed in version 2.x before 2.0.0.2.

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

**References:**

* BUGTRAQ: 20070226 rPSA-2007-0040-1 firefox
http://www.securityfocus.com/archive/1/archive/1/461336/100/0/threaded
* BUGTRAQ: 20070303 rPSA-2007-0040-3 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/461809/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-01.html
* MISC:
https://bugzilla.mozilla.org/show_bug.cgi?id=360645
* CONFIRM:
https://issues.rpath.com/browse/RPL-1081
* FEDORA: FEDORA-2007-281
http://fedoranews.org/cms/node/2713
* FEDORA: FEDORA-2007-293
http://fedoranews.org/cms/node/2728
* FEDORA: FEDORA-2007-308
http://fedoranews.org/cms/node/2747
* FEDORA: FEDORA-2007-309
http://fedoranews.org/cms/node/2749
* GENTOO: GLSA-200703-04
http://security.gentoo.org/glsa/glsa-200703-04.xml
* GENTOO: GLSA-200703-08
http://www.gentoo.org/security/en/glsa/glsa-200703-08.xml
* GENTOO: GLSA-200703-18
http://security.gentoo.org/glsa/glsa-200703-18.xml
* HP: HPSBUX02153
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00771742

* MANDRIVA: MDKSA-2007:052
http://www.mandriva.com/security/advisories?name=MDKSA-2007:052
* SLACKWARE: SSA:2007-066-03
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.374851
* SLACKWARE: SSA:2007-066-04
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.363947
* SLACKWARE: SSA:2007-066-05
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.338131
* SUSE: SUSE-SA:2007:019
http://lists.suse.com/archive/suse-security-announce/2007-Mar/0001.html
* SUSE: SUSE-SA:2007:022
http://www.novell.com/linux/security/advisories/2007_22_mozilla.html
* UBUNTU: USN-428-1
http://www.ubuntu.com/usn/usn-428-1
* UBUNTU: USN-431-1
http://www.ubuntu.com/usn/usn-431-1
* CERT-VN: VU#551436
http://www.kb.cert.org/vuls/id/551436

**CVE Reference:**

CVE-2007-0776 (cve.mitre.org, nvd.nist.gov)

- **16927 Mozilla Firefox JavaScript engine denial of service and arbitrary code execution Vulnerability (Remote File Checking)**

The JavaScript engine in Mozilla Firefox, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via certain vectors that trigger memory corruption.

The vulnerability is confirmed in version 1.5.0.x before 1.5.0.10 and 2.x before 2.0.0.2.

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

**References:**

* BUGTRAQ: 20070226 rPSA-2007-0040-1 firefox
http://www.securityfocus.com/archive/1/archive/1/461336/100/0/threaded
* BUGTRAQ: 20070303 rPSA-2007-0040-3 firefox thunderbird
http://www.securityfocus.com/archive/1/archive/1/461809/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-01.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-1081
* CONFIRM:
https://issues.rpath.com/browse/RPL-1103
* FEDORA: FEDORA-2007-281
http://fedoranews.org/cms/node/2713
* FEDORA: FEDORA-2007-293
http://fedoranews.org/cms/node/2728

* FEDORA: FEDORA-2007-308
http://fedoranews.org/cms/node/2747
* FEDORA: FEDORA-2007-309
http://fedoranews.org/cms/node/2749
* GENTOO: GLSA-200703-04
http://security.gentoo.org/glsa/glsa-200703-04.xml
* GENTOO: GLSA-200703-08
http://www.gentoo.org/security/en/glsa/glsa-200703-08.xml
* GENTOO: GLSA-200703-18
http://security.gentoo.org/glsa/glsa-200703-18.xml
* HP: HPSBUX02153
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00771742
* MANDRIVA: MDKSA-2007:050
http://www.mandriva.com/security/advisories?name=MDKSA-2007:050
* MANDRIVA: MDKSA-2007:052
http://www.mandriva.com/security/advisories?name=MDKSA-2007:052
* REDHAT: RHSA-2007:0079
http://www.redhat.com/support/errata/RHSA-2007-0079.html
* REDHAT: RHSA-2007:0077
http://rhn.redhat.com/errata/RHSA-2007-0077.html
* REDHAT: RHSA-2007:0078
http://www.redhat.com/support/errata/RHSA-2007-0078.html
* REDHAT: RHSA-2007:0097
http://www.redhat.com/support/errata/RHSA-2007-0097.html
* REDHAT: RHSA-2007:0108
http://www.redhat.com/support/errata/RHSA-2007-0108.html
* SGI: 20070301-01-P
ftp://patches.sgi.com/support/free/security/advisories/20070301-01-P.asc
* SGI: 20070202-01-P
ftp://patches.sgi.com/support/free/security/advisories/20070202-01-P.asc
* SLACKWARE: SSA:2007-066-03
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.374851
* SLACKWARE: SSA:2007-066-04
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.363947
* SLACKWARE: SSA:2007-066-05
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.338131
* SUSE: SUSE-SA:2007:019
http://lists.suse.com/archive/suse-security-announce/2007-Mar/0001.html
* SUSE: SUSE-SA:2007:022
http://www.novell.com/linux/security/advisories/2007_22_mozilla.html
* UBUNTU: USN-428-1
http://www.ubuntu.com/usn/usn-428-1
* UBUNTU: USN-431-1
http://www.ubuntu.com/usn/usn-431-1
* CERT-VN: VU#269484
http://www.kb.cert.org/vuls/id/269484
* BID: 22694
http://www.securityfocus.com/bid/22694
* FRSIRT: ADV-2007-0719
http://www.frsirt.com/english/advisories/2007/0719
* FRSIRT: ADV-2007-0718

http://www.frsirt.com/english/advisories/2007/0718
* FRSIRT: ADV-2008-0083
http://www.frsirt.com/english/advisories/2008/0083
* OSVDB: 32115
http://www.osvdb.org/32115
* SECTRACK: 1017698
http://www.securitytracker.com/id?1017698
* SECUNIA: 24238
http://secunia.com/advisories/24238
* SECUNIA: 24252
http://secunia.com/advisories/24252
* SECUNIA: 24287
http://secunia.com/advisories/24287
* SECUNIA: 24290
http://secunia.com/advisories/24290
* SECUNIA: 24205
http://secunia.com/advisories/24205
* SECUNIA: 24328
http://secunia.com/advisories/24328
* SECUNIA: 24333
http://secunia.com/advisories/24333
* SECUNIA: 24343
http://secunia.com/advisories/24343
* SECUNIA: 24320
http://secunia.com/advisories/24320
* SECUNIA: 24293
http://secunia.com/advisories/24293
* SECUNIA: 24393
http://secunia.com/advisories/24393
* SECUNIA: 24395
http://secunia.com/advisories/24395
* SECUNIA: 24384
http://secunia.com/advisories/24384
* SECUNIA: 24389
http://secunia.com/advisories/24389
* SECUNIA: 24410
http://secunia.com/advisories/24410
* SECUNIA: 24437
http://secunia.com/advisories/24437
* SECUNIA: 24522
http://secunia.com/advisories/24522
* SECUNIA: 24650
http://secunia.com/advisories/24650
* SECUNIA: 24406
http://secunia.com/advisories/24406
* SECUNIA: 24455
http://secunia.com/advisories/24455
* SECUNIA: 24456
http://secunia.com/advisories/24456
* SECUNIA: 24457
http://secunia.com/advisories/24457
* SECUNIA: 24342
http://secunia.com/advisories/24342
* XF: mozilla-multiple-javascript-code-execution(32699)
http://xforce.iss.net/xforce/xfdb/32699

**CVE Reference:**

CVE-2007-0777 (cve.mitre.org, nvd.nist.gov)

- **16928 Mozilla Firefox javascript: URI in HTML tags arbitrary JavaScript code execution Vulnerability (Remote File Checking)**

A regression error in Mozilla Firefox, allows remote attackers to execute arbitrary JavaScript as the user via an HTML mail message with a javascript: URI in an img, link, or style tag, which bypasses the access checks and executes code with chrome privileges.

The vulnerability is confirmed in version 2.x before 2.0.0.2 and 1.x before 1.5.0.10.

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

**References:**

* CONFIRM:
https://issues.rpath.com/browse/RPL-1103
* DEBIAN: DSA-1336
http://www.debian.org/security/2007/dsa-1336
* HP: HPSBUX02153
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00771742
* REDHAT: RHSA-2007:0078
http://www.redhat.com/support/errata/RHSA-2007-0078.html
* CONFIRM:
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=230733
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-09.html
* REDHAT: RHSA-2007:0097
http://www.redhat.com/support/errata/RHSA-2007-0097.html
* SGI: 20070301-01-P
ftp://patches.sgi.com/support/free/security/advisories/20070301-01-P.asc
* SLACKWARE: SSA:2007-066-03
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.374851
* SLACKWARE: SSA:2007-066-05
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.338131
* SUSE: SUSE-SA:2007:019
http://lists.suse.com/archive/suse-security-announce/2007-Mar/0001.html
* SUSE: SUSE-SA:2007:022
http://www.novell.com/linux/security/advisories/2007_22_mozilla.html
* BID: 22826
http://www.securityfocus.com/bid/22826
* FRSIRT: ADV-2007-0823
http://www.frsirt.com/english/advisories/2007/0823
* SECTRACK: 1017726
http://securitytracker.com/id?1017726
* SECUNIA: 24395
http://secunia.com/advisories/24395

* SECUNIA: 24384
http://secunia.com/advisories/24384
* SECUNIA: 24650
http://secunia.com/advisories/24650
* SECUNIA: 24455
http://secunia.com/advisories/24455
* SECUNIA: 24457
http://secunia.com/advisories/24457
* SECUNIA: 25588
http://secunia.com/advisories/25588

**CVE Reference:**

CVE-2007-0994 (cve.mitre.org, nvd.nist.gov)

- **16929 Mozilla Firefox layout engine Denial of Service Vulnerabilities (Remote File Checking)**

Multiple vulnerabilities in the layout engine for Mozilla Firefox, allow remote attackers to cause a denial of service (crash) via vectors related to dangling pointers, heap corruption, signed/unsigned, and other issues.

The vulnerability is confirmed in version 1.5.x before 1.5.0.12 and 2.x before 2.0.0.4.

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

**References:**

* BUGTRAQ: 20070531 FLEA-2007-0023-1: firefox
http://www.securityfocus.com/archive/1/archive/1/470172/100/200/threaded
* BUGTRAQ: 20070620 FLEA-2007-0027-1: thunderbird
http://www.securityfocus.com/archive/1/archive/1/471842/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-12.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-1424
* DEBIAN: DSA-1300
http://www.debian.org/security/2007/dsa-1300
* DEBIAN: DSA-1306
http://www.debian.org/security/2007/dsa-1306
* DEBIAN: DSA-1308
http://www.debian.org/security/2007/dsa-1308
* DEBIAN: DSA-1305
http://www.debian.org/security/2007/dsa-1305
* FEDORA: FEDORA-2007-308
http://fedoranews.org/cms/node/2747
* FEDORA: FEDORA-2007-309
http://fedoranews.org/cms/node/2749
* GENTOO: GLSA-200706-06
http://security.gentoo.org/glsa/glsa-200706-06.xml
* HP: HPSBUX02153
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00771742

* HP: HPSBUX02156
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00774579
* MANDRIVA: MDKSA-2007:119
http://www.mandriva.com/security/advisories?name=MDKSA-2007:119
* MANDRIVA: MDKSA-2007:120
http://www.mandriva.com/security/advisories?name=MDKSA-2007:120
* MANDRIVA: MDKSA-2007:131
http://www.mandriva.com/security/advisories?name=MDKSA-2007:131
* MANDRIVA: MDKSA-2007:126
http://www.mandriva.com/security/advisories?name=MDKSA-2007:126
* REDHAT: RHSA-2007:0400
http://www.redhat.com/support/errata/RHSA-2007-0400.html
* REDHAT: RHSA-2007:0401
http://www.redhat.com/support/errata/RHSA-2007-0401.html
* REDHAT: RHSA-2007:0402
http://www.redhat.com/support/errata/RHSA-2007-0402.html
* SLACKWARE: SSA:2007-066-04
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.363947
* SLACKWARE: SSA:2007-152-02
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.571857
* SUNALERT: 103136
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103136-1
* SUNALERT: 201532
http://sunsolve.sun.com/search/document.do?assetkey=1-66-201532-1
* SUSE: SUSE-SA:2007:036
http://www.novell.com/linux/security/advisories/2007_36_mozilla.html
* UBUNTU: USN-468-1
http://www.ubuntu.com/usn/usn-468-1
* UBUNTU: USN-469-1
http://www.ubuntu.com/usn/usn-469-1
* CERT: TA07-151A
http://www.us-cert.gov/cas/techalerts/TA07-151A.html
* CERT-VN: VU#751636
http://www.kb.cert.org/vuls/id/751636

**CVE Reference:**

CVE-2007-2867 (cve.mitre.org, nvd.nist.gov)

- **16930 Mozilla Firefox JavaScript engine Denial of Service and arbitrary code execution Vulnerabilities (Remote File Checking)**

Multiple vulnerabilities in the JavaScript engine for Mozilla Firefox, allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors that trigger memory corruption.

The vulnerability is confirmed in version 1.5.x before 1.5.0.12 and 2.x before 2.0.0.4.

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

**References:**

* BUGTRAQ: 20070531 FLEA-2007-0023-1: firefox
http://www.securityfocus.com/archive/1/archive/1/470172/100/200/threaded
* BUGTRAQ: 20070620 FLEA-2007-0027-1: thunderbird
http://www.securityfocus.com/archive/1/archive/1/471842/100/0/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-12.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-1424
* DEBIAN: DSA-1300
http://www.debian.org/security/2007/dsa-1300
* DEBIAN: DSA-1306
http://www.debian.org/security/2007/dsa-1306
* DEBIAN: DSA-1308
http://www.debian.org/security/2007/dsa-1308
* DEBIAN: DSA-1305
http://www.debian.org/security/2007/dsa-1305
* FEDORA: FEDORA-2007-308
http://fedoranews.org/cms/node/2747
* FEDORA: FEDORA-2007-309
http://fedoranews.org/cms/node/2749
* GENTOO: GLSA-200706-06
http://security.gentoo.org/glsa/glsa-200706-06.xml
* HP: HPSBUX02153
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00771742
* HP: HPSBUX02156
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00774579
* MANDRIVA: MDKSA-2007:119
http://www.mandriva.com/security/advisories?name=MDKSA-2007:119
* MANDRIVA: MDKSA-2007:120
http://www.mandriva.com/security/advisories?name=MDKSA-2007:120
* MANDRIVA: MDKSA-2007:131
http://www.mandriva.com/security/advisories?name=MDKSA-2007:131
* REDHAT: RHSA-2007:0400
http://www.redhat.com/support/errata/RHSA-2007-0400.html
* REDHAT: RHSA-2007:0401
http://www.redhat.com/support/errata/RHSA-2007-0401.html
* REDHAT: RHSA-2007:0402
http://www.redhat.com/support/errata/RHSA-2007-0402.html
* SLACKWARE: SSA:2007-066-04
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.363947
* SLACKWARE: SSA:2007-152-02
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.571857
* SUNALERT: 103125
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103125-1
* SUNALERT: 201505
http://sunsolve.sun.com/search/document.do?assetkey=1-66-201505-1
* SUSE: SUSE-SA:2007:036
http://www.novell.com/linux/security/advisories/2007_36_mozilla.html
* UBUNTU: USN-468-1

http://www.ubuntu.com/usn/usn-468-1
* UBUNTU: USN-469-1
http://www.ubuntu.com/usn/usn-469-1
* CERT: TA07-151A
http://www.us-cert.gov/cas/techalerts/TA07-151A.html
* CERT-VN: VU#609956
http://www.kb.cert.org/vuls/id/609956
* BID: 24242
http://www.securityfocus.com/bid/24242
* FRSIRT: ADV-2007-1994
http://www.frsirt.com/english/advisories/2007/1994
* FRSIRT: ADV-2007-3632
http://www.frsirt.com/english/advisories/2007/3632
* FRSIRT: ADV-2008-0082
http://www.frsirt.com/english/advisories/2008/0082
* SECTRACK: 1018151
http://www.securitytracker.com/id?1018151
* SECTRACK: 1018152
http://www.securitytracker.com/id?1018152
* SECTRACK: 1018153
http://www.securitytracker.com/id?1018153
* SECUNIA: 25476
http://secunia.com/advisories/25476
* SECUNIA: 25533
http://secunia.com/advisories/25533
* SECUNIA: 25496
http://secunia.com/advisories/25496
* SECUNIA: 25559
http://secunia.com/advisories/25559
* SECUNIA: 25635
http://secunia.com/advisories/25635
* SECUNIA: 25644
http://secunia.com/advisories/25644
* SECUNIA: 25647
http://secunia.com/advisories/25647
* SECUNIA: 25685
http://secunia.com/advisories/25685
* SECUNIA: 24406
http://secunia.com/advisories/24406
* SECUNIA: 24456
http://secunia.com/advisories/24456
* SECUNIA: 25534
http://secunia.com/advisories/25534
* SECUNIA: 25664
http://secunia.com/advisories/25664
* SECUNIA: 25469
http://secunia.com/advisories/25469
* SECUNIA: 25488
http://secunia.com/advisories/25488
* SECUNIA: 25489
http://secunia.com/advisories/25489
* SECUNIA: 25490
http://secunia.com/advisories/25490
* SECUNIA: 25491
http://secunia.com/advisories/25491

* SECUNIA: 25492
http://secunia.com/advisories/25492
* SECUNIA: 25750
http://secunia.com/advisories/25750
* SECUNIA: 25858
http://secunia.com/advisories/25858
* SECUNIA: 27427
http://secunia.com/advisories/27427
* SECUNIA: 28363
http://secunia.com/advisories/28363
* XF: mozilla-javascripteng-code-execution(34605)
http://xforce.iss.net/xforce/xfdb/34605

**CVE Reference:**

CVE-2007-2868 (cve.mitre.org, nvd.nist.gov)

- **16931 Mozilla Firefox addEventListener bypass the same-origin policy Vulnerability (Remote File Checking)**

Mozilla Firefox, allows remote attackers to bypass the same-origin policy and conduct cross-site scripting (XSS) and other attacks by using the addEventListener method to add an event listener for a site, which is executed in the context of that site.

The vulnerability is confirmed in version 1.5.x before 1.5.0.12 and 2.x before 2.0.0.4.

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

**References:**

* BUGTRAQ: 20070531 FLEA-2007-0023-1: firefox
http://www.securityfocus.com/archive/1/archive/1/470172/100/200/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-16.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-1424
* DEBIAN: DSA-1300
http://www.debian.org/security/2007/dsa-1300
* DEBIAN: DSA-1306
http://www.debian.org/security/2007/dsa-1306
* DEBIAN: DSA-1308
http://www.debian.org/security/2007/dsa-1308
* GENTOO: GLSA-200706-06
http://security.gentoo.org/glsa/glsa-200706-06.xml
* HP: HPSBUX02153
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00771742
* MANDRIVA: MDKSA-2007:120
http://www.mandriva.com/security/advisories?name=MDKSA-2007:120
* MANDRIVA: MDKSA-2007:126
http://www.mandriva.com/security/advisories?name=MDKSA-2007:126
* REDHAT: RHSA-2007:0400
http://www.redhat.com/support/errata/RHSA-2007-0400.html

* REDHAT: RHSA-2007:0402
http://www.redhat.com/support/errata/RHSA-2007-0402.html
* SLACKWARE: SSA:2007-152-02
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.571857
* SUSE: SUSE-SA:2007:036
http://www.novell.com/linux/security/advisories/2007_36_mozilla.html
* UBUNTU: USN-468-1
http://www.ubuntu.com/usn/usn-468-1
* CERT: TA07-151A
http://www.us-cert.gov/cas/techalerts/TA07-151A.html
* BID: 24242
http://www.securityfocus.com/bid/24242
* FRSIRT: ADV-2007-1994
http://www.frsirt.com/english/advisories/2007/1994
* SECTRACK: 1018160
http://www.securitytracker.com/id?1018160
* SECTRACK: 1018161
http://www.securitytracker.com/id?1018161
* SECUNIA: 25476
http://secunia.com/advisories/25476
* SECUNIA: 25533
http://secunia.com/advisories/25533
* SECUNIA: 25559
http://secunia.com/advisories/25559
* SECUNIA: 25635
http://secunia.com/advisories/25635
* SECUNIA: 25647
http://secunia.com/advisories/25647
* SECUNIA: 25685
http://secunia.com/advisories/25685
* SECUNIA: 25534
http://secunia.com/advisories/25534
* SECUNIA: 25469
http://secunia.com/advisories/25469
* SECUNIA: 25488
http://secunia.com/advisories/25488
* SECUNIA: 25490
http://secunia.com/advisories/25490
* SECUNIA: 25491
http://secunia.com/advisories/25491
* SECUNIA: 25750
http://secunia.com/advisories/25750
* SECUNIA: 25858
http://secunia.com/advisories/25858
* XF: mozilla-addeventlistener-xss(34614)
http://xforce.iss.net/xforce/xfdb/34614

**CVE Reference:**

CVE-2007-2870 (cve.mitre.org, nvd.nist.gov)

- **16932 Mozilla Firefox spoof or hide the browser chrome Vulnerability (Remote File Checking)**

Mozilla Firefox allows remote attackers to spoof or hide the browser chrome, such as the location bar, by placing XUL popups outside of the browser's content pane.

The vulnerability is confirmed in version 1.5.x before 1.5.0.12 and 2.x before 2.0.0.4.

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

**References:**

* BUGTRAQ: 20070531 FLEA-2007-0023-1: firefox
http://www.securityfocus.com/archive/1/archive/1/470172/100/200/threaded
* CONFIRM:
http://www.mozilla.org/security/announce/2007/mfsa2007-17.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-1424
* DEBIAN: DSA-1300
http://www.debian.org/security/2007/dsa-1300
* DEBIAN: DSA-1306
http://www.debian.org/security/2007/dsa-1306
* DEBIAN: DSA-1308
http://www.debian.org/security/2007/dsa-1308
* GENTOO: GLSA-200706-06
http://security.gentoo.org/glsa/glsa-200706-06.xml
* HP: HPSBUX02153
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00771742
* MANDRIVA: MDKSA-2007:120
http://www.mandriva.com/security/advisories?name=MDKSA-2007:120
* MANDRIVA: MDKSA-2007:126
http://www.mandriva.com/security/advisories?name=MDKSA-2007:126
* REDHAT: RHSA-2007:0400
http://www.redhat.com/support/errata/RHSA-2007-0400.html
* REDHAT: RHSA-2007:0401
http://www.redhat.com/support/errata/RHSA-2007-0401.html
* REDHAT: RHSA-2007:0402
http://www.redhat.com/support/errata/RHSA-2007-0402.html
* SLACKWARE: SSA:2007-152-02
http://slackware.com/security/viewer.php?l=slackware-security&y=2007&m=slackware-security.571857
* SUSE: SUSE-SA:2007:036
http://www.novell.com/linux/security/advisories/2007_36_mozilla.html
* UBUNTU: USN-468-1
http://www.ubuntu.com/usn/usn-468-1
* CERT: TA07-151A
http://www.us-cert.gov/cas/techalerts/TA07-151A.html
* BID: 24242
http://www.securityfocus.com/bid/24242
* FRSIRT: ADV-2007-1994
http://www.frsirt.com/english/advisories/2007/1994
* SECTRACK: 1018155
http://www.securitytracker.com/id?1018155
* SECTRACK: 1018156
http://www.securitytracker.com/id?1018156
* SECUNIA: 25476

http://secunia.com/advisories/25476
* SECUNIA: 25533
http://secunia.com/advisories/25533
* SECUNIA: 25559
http://secunia.com/advisories/25559
* SECUNIA: 25635
http://secunia.com/advisories/25635
* SECUNIA: 25647
http://secunia.com/advisories/25647
* SECUNIA: 25685
http://secunia.com/advisories/25685
* SECUNIA: 25534
http://secunia.com/advisories/25534
* SECUNIA: 25469
http://secunia.com/advisories/25469
* SECUNIA: 25488
http://secunia.com/advisories/25488
* SECUNIA: 25490
http://secunia.com/advisories/25490
* SECUNIA: 25491
http://secunia.com/advisories/25491
* SECUNIA: 25750
http://secunia.com/advisories/25750
* SECUNIA: 25858
http://secunia.com/advisories/25858
* XF: mozilla-xulpopups-spoofing(34606)
http://xforce.iss.net/xforce/xfdb/34606

**CVE Reference:**

CVE-2007-2871 (cve.mitre.org, nvd.nist.gov)

- **16933 Mozilla Firefox ..%5C sequences Directory traversal Vulnerability (Remote File Checking)**

Directory traversal vulnerability in Mozilla Firefox on Windows allows remote attackers to read arbitrary files via ..%5C (dot dot encoded backslash) sequences in a resource:// URI.

The vulnerability is confirmed in version 1.5.x before 1.5.0.12 and 2.x before 2.0.0.4.

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

**References:**

* BUGTRAQ: 20070604 Unpatched input validation flaw in Firefox 2.0.0.4
http://www.securityfocus.com/archive/1/archive/1/470500/100/0/threaded
* MISC:
http://ha.ckers.org/blog/20070516/read-firefox-settings-poc/
* MISC:
http://ha.ckers.org/blog/20070516/read-firefox-settings-poc/#comment-35888
* MISC:
http://larholm.com/2007/05/25/firefox-0day-local-file-reading/

* MISC:
http://larholm.com/2007/06/04/unpatched-input-validation-flaw-in-firefox-2004/
* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=367428
* SECUNIA: 25481
http://secunia.com/advisories/25481

**CVE Reference:**

CVE-2007-3072 (cve.mitre.org, nvd.nist.gov)

- **16934 Mozilla Firefox resource:// URI Directory traversal Vulnerability (Remote File Checking)**

Mozilla Firefox allows remote attackers to read files in the local Firefox installation directory via a resource:// URI.

The vulnerability is confirmed in version 1.5.x before 1.5.0.12 and 2.x before 2.0.0.4.

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

**References:**

* BUGTRAQ: 20070604 Unpatched input validation flaw in Firefox 2.0.0.4
http://www.securityfocus.com/archive/1/archive/1/470500/100/0/threaded
* MISC:
http://ha.ckers.org/blog/20070516/read-firefox-settings-poc/
* MISC:
http://larholm.com/2007/05/25/firefox-0day-local-file-reading/
* MISC:
http://larholm.com/2007/06/04/unpatched-input-validation-flaw-in-firefox-2004/
* MISC:
https://bugzilla.mozilla.org/show_bug.cgi?id=367428
* SECUNIA: 25481
http://secunia.com/advisories/25481

**CVE Reference:**

CVE-2007-3074 (cve.mitre.org, nvd.nist.gov)

# New Vulnerabilities found this Week

### IBM Lotus Domino 6 Web Server Cross-Site Scripting and Buffer Overflow

"Execution of arbitrary code"

Some vulnerabilities have been reported in IBM Lotus Domino, which can be exploited by malicious people to conduct cross-site scripting attacks or potentially compromise a vulnerable system.

1) A boundary error within the Lotus Domino Web Server can be exploited to cause a

stack-based buffer overflow via a specially crafted HTTP request with an overly long "Accept-Language" header.

Successful exploitation may allow execution of arbitrary code.

2) Certain unspecified input passed to the servlet engine/Web container is not properly sanitised before being used. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerabilities are reported in various 6.x versions.

References:
http://www-1.ibm.com/support/docview.wss?uid=swg21303057
http://www-1.ibm.com/support/docview.wss?uid=swg21303296

**GnuTLS Multiple Vulnerabilities**
"Denial of Service; execution of arbitrary code"

Some vulnerabilities have been reported in GnuTLS, which can be exploited by malicious people to cause a DoS (Denial of Service) or to potentially compromise an application using the library.

1) A boundary error exists in the processing "Client Hello" messages containing a "Server Name" extension. This can be exploited to cause a heap-based buffer overflow via a specially crafted TLS packet.

Successful exploitation may allow execution of arbitrary code.

2) A NULL-pointer dereference error in the processing of TLS packets containing multiple "Client Hello" messages can be exploited to crash an affected application.

3) A signedness error exists within the "_gnutls_ciphertext2compressed()" function in lib/gnutls_cipher.c. This can be exploited to cause an out of bounds read and crash an affected application via specially crafted, encrypted TLS data.

The vulnerabilities are reported in versions prior to 2.2.4.

References:
http://www.cert.fi/haavoittuvuudet/advisory-gnutls.html
http://lists.gnu.org/archive/html/gnutls-devel/2008-05/msg00060.html

**Stunnel Windows Privilege Escalation Vulnerability**
"Gain escalated privileges"

A vulnerability has been reported in Stunnel, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to an unspecified error when Stunnel is running as a Windows service. This can be exploited to run arbitrary commands with LocalSystem privileges.

The vulnerability is reported in versions prior to 4.23.

References:
http://www.stunnel.org/news/

### Cisco Unified Presence SIP Proxy Service Denial of Service

"Denial of Service"

A vulnerability has been reported in Cisco Unified Presence, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the SIP Proxy service and can be exploited to cause a DoS condition when e.g. performing a TCP port scan on an affected system.

The vulnerability affects versions 6.0(1) and 6.0(2).

References:
http://www.cisco.com/warp/public/707/cisco-sa-20080514-cup.shtml

### Linux Kernel Multiple Vulnerabilities

"Denial of service; crash the system"

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

1) An error exists in the implementation of the "sys_utimensat()" system call. This can be exploited to update the access or modification time of arbitrary files via specially crafted arguments passed to the affected system call.

2) A memory leak exists in the "ipip6_rcv()" function included in the IPv6 over IPv4 (SIP) tunneling driver. This can be exploited to potentially exhaust all available memory via specially crafted network packets.

3) An error when checking "mmap()" address limits on SPARC platforms can be exploited to crash the system.

The vulnerabilities are reported in version 2.6.25.2. Prior versions may also be affected.

References:
http://marc.info/?l=linux-netdev&m=121030861218192&w=2

### 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