netVigilance

**ScoutNews Team** **31st December 2004**
**Issue #53**

Weekly ScoutNews by netVigilance

**Table of Contents**



# This Week in Review

Happy New Year 2005,

---oooo---

As we greet the New Year our hearts go out to the Millions of people who have had their lives altered by the Tsunami's these Holidays. We at netVigilance are donating to the help, and urge you and your organizations to donate as well.

---oooo---

We have dubbed 2004 the year of the worm, however myriad more things are going on. Many companies are consolidating in their efforts to become the one stop shop for IT security. At the same time we see the malicious activities gear up in speed and intelligence faster than any one organization can get its thoughts around what a prudent defense strategy should be.

This week's choice of stories underlines the dynamics in the IT security challenge that lies ahead.

Enjoy reading and see you in 2005

# Top Security News Stories this Week

- **Phishing, Spyware, Others Plague Internet**
  Computer worms raced around the world, leaving behind tools that spread spam. Scammers sent e-mail to trick bank account holders into revealing passwords. Rogue programs known as "spyware" hijacked Web browsers and crippled computers. These were among the top Internet threats of 2004 as the perpetrators grew smarter and more sophisticated, driven more than ever by economic gains. And while technology to combat such threats has improved, experts concede that's not enough to address what's bound to emerge in the coming year.

http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738&e=2&u=/ap/20041231/ap_on_hi_te/internet_security
Anick Jesdanun

❖ **Five Years Later, Windows 2000 Looks Naïve**

I remember roughly when Windows 2000 (news - web sites) "went gold"—when Microsoft finalized the shipping code for the product. It was mid-December 1999, and the product officially "shipped" in February 2000. I was writing part of a Windows 2000 book so I had early access.

Five years ago is a long, long time in this day and age, especially when it comes to security. A lot has happened since then, and things are far worse now than they were. Can we forgive Microsoft for being naïve about security in Windows 2000? I might have thought so at one point, but not anymore.

Yes, the real work on Windows 2000 was done as the Internet boom was at its most stupid, with people selling groceries online and Fedexing bags of dog food, but Microsoft wasn't that kind of company. It was run by experienced people who should have known better.

http://story.news.yahoo.com/news?tmpl=story&cid=1738&ncid=1208&e=6&u=/zd/20041230/tc_zd/141766
Larry Seltzer

❖ **Computer viruses morphing, with no end in sight**

Use protection. Please.

It's a message people like Ryan Kokai try to knock into the heads of family, buddies and co-workers time and time again.

And he's not talking about sex. In his role as tech wizard, the 25-year-old is frequently called away from his desk to clean up co-workers' computers which have been infected with viruses or other troublesome computer ailments. He makes housecalls in the evenings and on weekends for his friends -- and sometimes friends of friends.

http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1104435120700_50/?hub=SciTech
Canaidian Press

❖ **2004: The Changing Face of Spam**

Despite government and industry efforts to stop spam, the U.S. remains the world's largest source of unwanted e-mail, which now represents some 90 percent of all Web traffic. Experts see little hope of stemming the tide.

The United States was the biggest source country for spammed messages in 2004 -- as it was the previous year.

The passage of the much-ballyhooed CAN-SPAM act in January apparently made little dent in the volume of spam, which is now thought to make up 90 percent of all Internet traffic.

It would seem that little has changed in the war against spam, except perhaps its means and motivations -- malware and money; developments that are hardly welcomed by the Internet community.

http://www.cio-today.com/story.xhtml?story_title=------The-Changing-Face-of-Spam&story_id=29397&category=cybercrime

Erika Morphy

# New Vulnerabilities Tested in SecureScout

- **14670 Mozilla "MSG_UnEscapeSearchUrl()" Buffer Overflow Vulnerability (Remote File Checking)**

Maurycy Prodeus has reported a vulnerability in Mozilla.

The vulnerability is caused due to a boundary error in the "MSG_UnEscapeSearchUrl()" function in "nsNNTPProtocol.cpp" when processing NNTP URIs. This can be exploited via e.g. a malicious web site to cause a heap-based buffer overflow when referencing a specially crafted, overly long "news://" URI.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 1.7.3 and prior.

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

**CVE Links:**

**Reference:** https://bugzilla.mozilla.org/show_bug.cgi?id=264388 & http://www.isec.pl/vulnerabilities/isec-0020-mozilla.txt

- **14671 Mozilla Window Injection Vulnerability (Remote File Checking)**

Secunia Research has reported a vulnerability in Mozilla, which can be exploited by malicious people to spoof the content of websites.

The problem is that a website can inject content into another site's window if the target name of the window is known. This can e.g. be exploited by a malicious website to spoof the content of a pop-up window opened on a trusted website.

Secunia has constructed a test, which can be used to check if your browser is affected by this issue:
http://secunia.com/multiple_browsers_window_injection_vulnerability_test/

The vulnerability has been confirmed in Mozilla 1.7.3. Other versions may also be affected.

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

**CVE Links:** CAN-2004-1156

**Reference:** http://secunia.com/secunia_research/2004-13/advisory/

- **14672 Mozilla Tabbed Browsing Vulnerabilities (Remote File Checking)**

Secunia Research has discovered two vulnerabilities in Mozilla which can be exploited by malicious web sites to obtain sensitive information and spoof dialog boxes.

1) Inactive tabs can launch dialog boxes so they appear to be displayed by a web site in

another tab. This can be exploited by a malicious web site to show a dialog box, which seems to originate from a trusted web site.

Successful exploitation would normally require that a user is tricked into opening a link from a malicious web site to a trusted web site in a new tab.

A test is available here:
http://secunia.com/multiple_browsers_dialog_box_spoofing_test/

The vulnerability has been confirmed in the following versions:
* Mozilla 1.7.2 and 1.7.3

2) Inactive tabs can gain focus from form fields on web sites in another tab. This can potentially be exploited to collect sensitive data entered in form fields on other web sites.

Successful exploitation would normally require that a user is tricked into opening a link from a malicious web site to a trusted web site in a new tab.

A test is available here:
http://secunia.com/multiple_browsers_form_field_focus_test/

The vulnerability has been confirmed in the following versions:
* Mozilla 1.7.2 and 1.7.3

Other versions may also be vulnerable.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: M**edium**

**CVE Links:**

**Reference:** http://secunia.com/secunia_research/2004-10/ &
https://bugzilla.mozilla.org/show_bug.cgi?id=262887

- **14673 Mozilla Firefox Tabbed Browsing Vulnerabilities (Remote File Checking)**

Secunia Research has discovered two vulnerabilities in Mozilla which can be exploited by malicious web sites to obtain sensitive information and spoof dialog boxes.

1) Inactive tabs can launch dialog boxes so they appear to be displayed by a web site in another tab. This can be exploited by a malicious web site to show a dialog box, which seems to originate from a trusted web site.

Successful exploitation would normally require that a user is tricked into opening a link from a malicious web site to a trusted web site in a new tab.

A test is available here:
http://secunia.com/multiple_browsers_dialog_box_spoofing_test/

The vulnerability has been confirmed in the following versions:
* Mozilla Firefox 0.10.1
* Mozilla Firefox 1.0 (affected by variant)

2) Inactive tabs can gain focus from form fields on web sites in another tab. This can potentially be exploited to collect sensitive data entered in form fields on other web sites.

Successful exploitation would normally require that a user is tricked into opening a link from a malicious web site to a trusted web site in a new tab.

A test is available here:
http://secunia.com/multiple_browsers_form_field_focus_test/

The vulnerability has been confirmed in the following versions:
* Mozilla Firefox 0.10.1

Other versions may also be vulnerable.

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

**CVE Link:**

**Reference:** http://secunia.com/secunia_research/2004-10/ & https://bugzilla.mozilla.org/show_bug.cgi?id=262887

- **14674 Mozilla Firefox Download Directory File Deletion Vulnerability (Remote File Checking)**

Alex Vincent has reported a vulnerability in Mozilla Firefox, which can be exploited by malicious people to delete files on a user's system.

The vulnerability is caused due to an error when downloading files and can be exploited to delete all content in the download directory (by default the user's desktop on Windows and the user's $HOME directory on Linux).

Successful exploitation requires that a user is tricked into clicking the "Save" button to download a file.

The vulnerability affects versions up to 0.10.1. not included.

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

**CVE Link:**

**Reference:** http://www.mozilla.org/projects/security/known-vulnerabilities.html#firefox0.10.1 & https://bugzilla.mozilla.org/show_bug.cgi?id=259708

- **14675 Mozilla Firefox Window Injection Vulnerability (Remote File Checking)**

Secunia Research has reported a vulnerability in Mozilla Firefox, which can be exploited by malicious people to spoof the content of websites.

The problem is that a website can inject content into another site's window if the target name of the window is known. This can e.g. be exploited by a malicious website to spoof the content of a pop-up window opened on a trusted website.

Secunia has constructed a test, which can be used to check if your browser is affected by this issue:

http://secunia.com/multiple_browsers_window_injection_vulnerability_test/

The vulnerability has been confirmed in Mozilla Firefox 1.0. Other versions may also be affected.

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

**CVE Link:** CAN-2004-1156

**Reference:** http://secunia.com/secunia_research/2004-13/advisory/ & https://bugzilla.mozilla.org/show_bug.cgi?id=273699

- **15555 Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdy38035)**
  The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

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

**CVE Link:** CAN-2002-1103

**Reference:**
http://www.cisco.com/en/US/products/products_security_advisory09186a00800c8154.shtml

- **19309 Hijack ShopForGood**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://www.pestpatrol.com/PestInfo/s/shopforgood.asp

- **19310 Hijack SiteHistory**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://www.pestpatrol.com/PestInfo/s/sitehistory.asp

- **19311 Hijack SmartBrowser**
  Hijacker: Any software that resets your browser's settings to point to other sites. Hijacks

may reroute your info and address requests through an unseen site, capturing that info. In such hijacks, your browser may behave normally, but be slower. Homepage Hijackers will change your home page to some other site. Error Hijackers will display a new error page when a requested URL is not found.

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

**CVE Link:** GENERIC-MAP-NOMATCH

**Reference:** http://www.pestpatrol.com/PestInfo/s/smartbrowser.asp

# New Vulnerabilities found this Week

- **Mozilla "MSG_UnEscapeSearchUrl()" Buffer Overflow Vulnerability**

Maurycy Prodeus has reported a vulnerability in Mozilla, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the "MSG_UnEscapeSearchUrl()" function in "nsNNTPProtocol.cpp" when processing NNTP URIs. This can be exploited via e.g. a malicious web site to cause a heap-based buffer overflow when referencing a specially crafted, overly long "news://" URI.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in version 1.7.3 and prior.

References:
https://bugzilla.mozilla.org/show_bug.cgi?id=264388
http://www.isec.pl/vulnerabilities/isec-0020-mozilla.txt

- **Netcat "SessionWriteShellThreadFn()" Buffer Overflow Vulnerability**

class101 has reported a vulnerability in Netcat for Windows, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the "SessionWriteShellThreadFn()" function in "doexec.c" when writing to a pipe connected to a shell process. This can be exploited to cause a buffer overflow by sending specially crafted overly long data to a listening port.

Successful exploitation allows execution of arbitrary code, but requires that Netcat has been invoked with the "-e" command line option.

NOTE: Exploit code has been published on a public mailing list.

The vulnerability has been reported in version 1.1. Prior versions may also be affected.

References:
http://www.vulnwatch.org/netcat/netcat-111.txt
http://www.hat-squad.com/en/000142.html

- **Linux Kernel SACF Instruction Privilege Escalation Vulnerability**

Martin Schwidefsky has reported a vulnerability in the Linux Kernel, which can be exploited by malicious, local users to gain escalated privileges.

The vulnerability is caused due to the SACF (Set Address Space Control Fast) control instruction being handled insecurely on the S/390 platform.

- **Linux Security Modules Running Processes Capability Security Issue**

LiangBin has reported a security issue in Linux Security Modules (LSM), which may grant normal user processes escalated privileges.

The problem is that when loading the Capability LSM module as a loadable kernel module, all existing processes gain unintended capabilities granting them root privileges.

- **Perl "File::Path::rmtree" Race Condition**

Paul Szabo has reported a vulnerability in Perl "File::Path::rmtree", allowing malicious, local users to gain escalated privileges.

The vulnerability is caused due to a race condition in the way "File::Path::rmtree" changes permissions on files before deleting them. This can be exploited by creating a symbolic link to arbitrary files.

Successful exploitation may allow changing permissions or removing arbitrary files, if root uses an application using the vulnerable code to delete files.

References:
http://secunia.com/advisories/13643/

- **Snort TCP/IP Options Denial of Service Vulnerability**

Marcin Zgorecki has reported a vulnerability in Snort, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the printing of TCP/IP options. This can be exploited to cause an unspecified DoS by sending a specially crafted packet.

Successful exploitation requires that snort is configured with "FAST" output or verbose mode.

The vulnerability has been reported in version 2.2.10. Other versions may also be affected.

References:
http://www.snort.org/dl/

**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