netVigilance
assurance has arrived

# ScoutNews

*The weekly Security update from the makers of SecureScout*

2007 Issue # 23

June 15, 2007

**Table of Contents**



## Product Focus

**RPC DCOM Vulnerabilities Scanner** – The RPC DCOM Vulnerabilities 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 Windows RPC DCOM flaws (MS03-026 and MS03-039).

## This Week in Review

University didn't notice hack for 2 years. "Operation Bot Roast" giving results. Apple and security.California ruling expected to have great impact on web privacy.

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

- **University fails to notice hack attack**

Attack at University of Virginia goes undetected for two years

Faculty members at the University of Virginia have had their personal records hacked, including salary details and social security numbers.

The hack, which is believed to have gone undetected for two years, netted details on over 6,000 staff who had taught at the university from 1990 to August 2003.

The hacker defaced a web page on the university's portal and when IT staff cleaned up they found evidence of the attack.

"We sincerely regret the distress this causes to our colleagues," said James Hilton, vice president and chief information officer at the University of Virginia.

vnunet

Full Story :
http://www.vnunet.com/vnunet/news/2192038/university-virginia-hacked

### ❖ FBI nabs three 'bot herders'

Among them was a hacker who infected Chicago hospital systems
The FBI yesterday announced that its "Operation Bot Roast" anti-botnet sweep has so far identified more than 1 million hijacked personal computers and resulted in the arrest of three men charged with everything from spamming to infecting systems at several hospitals.

The operation is an ongoing effort to disrupt the bot trade and identify botnet controllers, the FBI said at a news conference. "Bot" is the term for an infected personal computer. A "botnet" is a large number of hijacked PCs controlled by a hacker, called a "bot herder." Botnets are used by spammers, criminals launching distributed-denial-of-service (DDoS) attacks and malware authors looking to spread their applications.

"The majority of victims are not even aware that their computer has been compromised or their personal information exploited," James Finch, FBI assistant director for the cyber division, said in a statement.

computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9024720&taxonomyId=17&intsrc=kc_top

### ❖ Apple Goes on Safari With Hostile Security Researchers

Security researchers have long speculated that Apple has benefited from security by obscurity, escaping attention from malicious hackers because Windows-based computers dominate in homes and offices. But Apple's new Safari for Windows puts it right in hackers' cross hairs. The browser gives hackers another way to attack Windows and security researchers will now likely spend hours hunting down holes in the code.

But Apple's culture of secrecy and slick marketing has put it at odds with a community that values openness and honesty -- a lot of computer security experts aren't very fond of the computer maker.

Indeed some in the security community think Apple's stance towards security is as bad as Microsoft's was in the days when it was called the "Evil Empire," prior to Bill Gates' declaration in 2002 that security was the company's top priority.

wired

Full Story :
http://www.wired.com/gadgets/mac/news/2007/06/researchersmeetsafari

- **TorrentSpy ruling a 'weapon of mass discovery'**

It was a pro-copyright ruling that stunned nearly everyone dealing with the issue of online piracy.
In a decision reported late Friday by CNET News.com, a federal judge in Los Angeles found (PDF) that a computer server's RAM, or random-access memory, is a tangible document that can be stored and must be turned over in a lawsuit.

If allowed to stand, the groundbreaking ruling may mean that anyone defending themselves in a civil suit could be required to turn over information in their computer's RAM hardware, which could force companies and individuals to store vast amounts of data, say technology experts. Roaming the Web anonymously was already nearly impossible. This ruling, which brings up serious privacy issues, could make it a lot harder.

Cnet news

Full Story :
http://news.com.com/TorrentSpy+ruling+a+weapon+of+mass+discovery/2100-1030_3-6190900.html?tag=newsmap

# New Vulnerabilities Tested in SecureScout

- **16525 Content Disposition Parsing Cross Domain Information Disclosure Vulnerability (MS07-034/929123) (Remote File Checking)**

An information disclosure vulnerability exists in the way MHTML protocol handler passes Content-Disposition notifications back to Internet Explorer. The vulnerability could allow an attacker to bypass the file download dialog box in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If the user viewed the Web page using Internet Explorer, the vulnerability could potentially allow information disclosure. An attacker who successfully exploited this vulnerability could read data from another Internet Explorer domain.

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

**References:**

Original advisory:
* MS:MS07-034
http://www.microsoft.com/technet/security/bulletin/ms07-034.mspx

**CVE Reference:** CVE-2007-2227

### ❖ 16524 URL Parsing Cross Domain Information Disclosure Vulnerability (MS07-034/929123) (Remote File Checking)

An information disclosure vulnerability exists in Windows because the MHTML protocol handler incorrectly interprets HTTP headers when returning MHTML content. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If the user viewed the Web page using Internet Explorer, the vulnerability could potentially allow information disclosure. An attacker who successfully exploited this vulnerability could read data from another Internet Explorer domain.

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

**References:**

Original advisory:
* MS:MS07-034
http://www.microsoft.com/technet/security/bulletin/ms07-034.mspx

**CVE Reference:** CVE-2007-2225

### ❖ 16523 Windows Mail UNC Navigation Request Remote Code Execution Vulnerability (MS07-034/929123) (Remote File Checking)

A remote code execution vulnerability results from the way local or UNC navigation requests are handled in Windows Mail. An attacker could exploit the vulnerability by constructing a specially crafted e-mail message that could potentially allow execution of code from a local file or UNC path if a user clicked on a link in the e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
* MS:MS07-034
http://www.microsoft.com/technet/security/bulletin/ms07-034.mspx

Other references:
# FULLDISC:20070323 Microsoft Windows Vista - Windows Mail Client Side Code Execution Vulnerability
# URL:http://archives.neohapsis.com/archives/fulldisclosure/2007-03/0344.html
# FULLDISC:20070323 Re: Microsoft Windows Vista - Windows Mail Client Side Code Execution Vulnerability
# URL:http://archives.neohapsis.com/archives/fulldisclosure/2007-03/0345.html
# FULLDISC:20070323 Re: Microsoft Windows Vista - Windows Mail Client Side Code Execution Vulnerability
# URL:http://archives.neohapsis.com/archives/fulldisclosure/2007-03/0346.html
# BID:23103
# URL:http://www.securityfocus.com/bid/23103
# XF:windows-mail-code-execution(33167)
# URL:http://xforce.iss.net/xforce/xfdb/33167

**CVE Reference:** CVE-2007-1658

### ❖ 16522 URL Redirect Cross Domain Information Disclosure Vulnerability (MS07-034/929123) (Remote File Checking)

An information disclosure vulnerability exists in Windows because the MHTML protocol handler incorrectly interprets the MHTML URL redirections that could potentially bypass Internet Explorer domain restrictions. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If the user viewed the Web page using Internet Explorer, the vulnerability could potentially allow information disclosure. An attacker who successfully exploited this vulnerability could read data from another Internet Explorer domain.

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

**References:**

Original advisory:
* MS:MS07-034
http://www.microsoft.com/technet/security/bulletin/ms07-034.mspx

Other references:
# BUGTRAQ:20061025 IE7 status: 8 days after release, 3 unfixed issues
# URL:http://www.securityfocus.com/archive/1/archive/1/449917/100/0/threaded
# BUGTRAQ:20061026 IE7 is a Source of Problem - Secunia IE7 Release Incident of October 2006
# URL:http://www.securityfocus.com/archive/1/archive/1/449883/100/200/threaded
# MISC: http://secunia.com/Internet_Explorer_Arbitrary_Content_Disclosure_Vulnerability_Test/
# BID:17717
# URL:http://www.securityfocus.com/bid/17717
# FRSIRT:ADV-2006-1558
# URL:http://www.frsirt.com/english/advisories/2006/1558

# OSVDB:25073
# URL:http://www.osvdb.org/25073
# SECTRACK:1016005
# URL:http://securitytracker.com/id?1016005
# SECUNIA:19738
# URL:http://secunia.com/advisories/19738
# SECUNIA:22477
# URL:http://secunia.com/advisories/22477
# XF:ie-mhtml-information-disclosure(26281)
# URL:http://xforce.iss.net/xforce/xfdb/26281

**CVE Reference:** CVE-2006-2111

### ❖ 16521 Internet Explorer Speech Control Memory Corruption Vulnerability (MS07-033/933566) (Remote File Checking)

A remote code execution vulnerability exists in a component of Microsoft Speech API 4. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
* MS:MS07-033
http://www.microsoft.com/technet/security/bulletin/ms07-033.mspx

**CVE Reference:** CVE-2007-2222

### ❖ 16520 Internet Explorer Navigation Cancel Page Spoofing Vulnerability (MS07-033/933566) (Remote File Checking)

A spoofing vulnerability exists in Internet Explorer that could allow an attacker to display spoofed content in the Navigation canceled page. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
* MS:MS07-033
http://www.microsoft.com/technet/security/bulletin/ms07-033.mspx

Other references:
# BUGTRAQ:20070314 Phishing using IE7 local resource vulnerability
# URL:http://www.securityfocus.com/archive/1/archive/1/462833/100/0/threaded
# BUGTRAQ:20070315 RE: Phishing using IE7 local resource vulnerability
# URL:http://www.securityfocus.com/archive/1/archive/1/462945/100/0/threaded
# BUGTRAQ:20070315 Re: Phishing using IE7 local resource vulnerability
# URL:http://www.securityfocus.com/archive/1/archive/1/462939/100/0/threaded
# MISC:
http://aviv.raffon.net/2007/03/14/PhishingUsingIE7LocalResourceVulnerability.aspx
# MISC: http://news.com.com/2100-1002_3-6167410.html
# FRSIRT:ADV-2007-0946
# URL:http://www.frsirt.com/english/advisories/2007/0946
# SECUNIA:24535
# URL:http://secunia.com/advisories/24535
# XF:ie-navcancl-xss(33026)
# URL:http://xforce.iss.net/xforce/xfdb/33026

**CVE Reference:** CVE-2007-1499

### ❖ 16519 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS07-033/933566) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or that has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
* MS:MS07-033
http://www.microsoft.com/technet/security/bulletin/ms07-033.mspx

**CVE Reference:** CVE-2007-1751

### ❖ 16518 Internet Explorer Language Pack Installation Vulnerability (MS07-033/933566) (Remote File Checking)

A remote code execution vulnerability exists in Internet Explorer in the way that it handles language pack installation. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system. User interaction, while expected, is required to exploit this vulnerability.

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

**References:**

Original advisory:
* MS:MS07-033
http://www.microsoft.com/technet/security/bulletin/ms07-033.mspx

**CVE Reference:** CVE-2007-3027

❖ **16517 Internet Explorer CSS Tag Memory Corruption Vulnerability (MS07-033/933566) (Remote File Checking)**

A remote code execution vulnerability exists in Internet Explorer due to improper handling of a CSS tag. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
* MS:MS07-033
http://www.microsoft.com/technet/security/bulletin/ms07-033.mspx

**CVE Reference:** CVE-2007-1750

❖ **16516 Internet Explorer COM Object Instantiation Memory Corruption Vulnerability (MS07-033/933566) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

Original advisory:
* MS:MS07-033
http://www.microsoft.com/technet/security/bulletin/ms07-033.mspx

**CVE Reference:** CVE-2007-0218

# New Vulnerabilities found this Week

## Microsoft Patch Tuesday

"Code execution; Information Disclosure"

Microsoft released a series of patches to address the following security issues:

Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)
Cumulative Security Update for Internet Explorer (933566)
Cumulative Security Update for Outlook Express and Windows Mail (929123)
Vulnerability in Win32 API Could Allow Remote Code Execution (935839)
Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (927051)
Vulnerability in Windows Vista Could Allow Information Disclosure (931213)

References:
http://www.microsoft.com/technet/security/bulletin/ms07-030.mspx
http://www.microsoft.com/technet/security/bulletin/ms07-031.mspx
http://www.microsoft.com/technet/security/bulletin/ms07-032.mspx
http://www.microsoft.com/technet/security/bulletin/ms07-033.mspx
http://www.microsoft.com/technet/security/bulletin/ms07-034.mspx
http://www.microsoft.com/technet/security/bulletin/ms07-035.mspx
http://descriptions.securescout.com/tc/16516
http://descriptions.securescout.com/tc/16517
http://descriptions.securescout.com/tc/16518
http://descriptions.securescout.com/tc/16519
http://descriptions.securescout.com/tc/16520
http://descriptions.securescout.com/tc/16521
http://descriptions.securescout.com/tc/16522
http://descriptions.securescout.com/tc/16523
http://descriptions.securescout.com/tc/16524
http://descriptions.securescout.com/tc/16525

## libexif EXIF Information Integer Overflow Vulnerability

"Denial of Service"

A vulnerability has been reported in libexif, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise an application using the library.

The vulnerability is caused due to an integer overflow error within the "exif_data_load_data_entry()" function when handling EXIF component information and can be exploited to cause a heap based buffer overflow.

Successful exploitation may allow an attacker to crash an application using the library or to execute arbitrary code.

The vulnerability is reported in versions prior to 0.6.16.

References:
http://sourceforge.net/project/shownotes.php?release_id=515385
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=543

## OpenOffice RTF File and FreeType Font Parsing Vulnerabilities

“Code execution”

Some vulnerabilities have been reported in OpenOffice, which can potentially be exploited by malicious people to compromise a user's system.

1) An error exists when parsing the "prdata" tag in RTF files where the first token is smaller that the second one. This can be exploited to cause a heap-based buffer overflow by e.g. tricking a user into opening a specially crafted RTF files.

2) A vulnerability is caused due to the use of a vulnerable copy of the FreeType library, which can be exploited to cause a heap based buffer overflow by e.g. tricking a user into opening a specially crafted document.

Successful exploitation may allow the execution of arbitrary code.

References:
http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-openoffice-rtf-document-handling/
http://www.openoffice.org/security/CVE-2007-0245.html
http://www.openoffice.org/security/CVE-2007-2754.html
http://www.us.debian.org/security/2007/dsa-1307

**Sun Java System Products NSS SSLv2 Processing Buffer Overflows**
“Code execution”

Sun has acknowledged some vulnerabilities in various Sun Java System products, which potentially can be exploited by malicious people to compromise a vulnerable system.

Note: SSLv2 is disabled by default in the Sun Java System Application Server, Sun Java System Web Server, and Sun Java System Web Proxy Server.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102945-1

**Linux Kernel Multiple Vulnerabilities**
“Denial of Service”

Two vulnerabilities and a weakness have been reported in the Linux Kernel, which can be exploited by malicious, local users to disclose potentially sensitive information and malicious people to cause a DoS (Denial of Service).

1) A NULL-pointer dereference exists within netfilter when handling new SCTP connections with unknown chunk types. This can be exploited to crash the kernel by sending malicious packets.

2) An underflow error within the "cpuset_task_read()" function in /kernel/cpuset.c can be exploited to read kernel memory, which may contain potentially sensitive information.

Successful exploitation requires that the attacker has access to open the /dev/cpuset/tasks file (the cpuset file system needs to be mounted).

3) The kernel does not handle seeds for the random number generator correctly. This may weaken the security of applications relying on the randomness of the kernel random

number generator.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21.4
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=541

**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