netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 49

December 14, 2007

Table of Contents

Product Focus

Spida Digispid Worm Scanner – The Spida Digispid Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are prone any of the Microsoft Java Virtual Machine Vulnerabilities (MS02-069).

This Week in Review

iPhone predicted major target next year. SANS looking at security successes in federal government. Spam: It seemed like a good idea at the time. Data breaches discussion.

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

- **iPhone will be Primary Target for Hackers in 2008**

Security predictions released by Arbor Networks reveals that the iPhone will be a major target for cybercriminals in 2008. The forecast also highlights Chinese specific crime as a major issue for the New Year.

Arbor's Security and Engineering Response Team (ASERT), who have put together the forecasts, believe that the iPhone will become the victim of a serious attack in 2008. These assaults are likely to be in the form of drive by attacks – malware embedded

into seemingly harmless information, images or other media that actually perform dangerous actions when rendered on the iPhone's Web browser. With the scrutiny the iPhone has received since its launch earlier this year over network lock-in, ASERT believes that hackers will be enticed by the possibility of attacking Apple users and the opportunity to "be the first" to hack a new platform.

XTVWorld

Full Story :
http://press.xtvworld.com/article22200.html

❖ Six federal security programs that are making a difference

SANS list turns up a half-dozen success stories in government
When it comes to information security issues, the stories that get the most ink are usually the ones about massive data breaches and other foul-ups, especially if they occur within government.

That's one of the reasons why the Bethesda, Md.-based SANS Institute has decided to come out with a list that focuses on what it considers to be some of the more successful security efforts within the federal government. "It gets old if all you ever do is take potshots" at entities that suffer breaches, said Alan Paller, SANS' director of research.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9052899&intsrc=hm_list

❖ Unsung innovators: Gary Thuerk, the father of spam

It seemed like a good idea at the time, back before junk e-mail even had a nickname, no less a place in computer history.

"I knew I was pushing the envelope," says Gary Thuerk, who on May 1, 1978, sent out the first unsolicited mass e-mailing in history. "I thought of it as e-marketing," he says about that first spam message, sent pre-Internet and two decades before most Americans were even getting their first e-mail address. "We wanted to reach as many as people as possible to let them know about our new product. It was coming out Dec. 20 of that year, and we didn't want to send invitations."

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&articleId=9046419&taxonomyId=82&intsrc=kc_feat

❖ IT lapses

Stories of 'yet another IT security lapse by company X' are hitting the headlines far too

often, each time raising the alarm about how little is being done to protect commercially sensitive data on mobile devices and the hidden costs associated with this negligence. Some recent victims of laptop security breaches include organisations in the retail, banking, public sector and local government markets. One local council had an employee laptop, containing the personal details of staff and former personnel, stolen during a street robbery. The council subsequently notified all affected staff and set up a hotline offering advice on how to protect themselves from potential identify theft.

Professional Security

Full Story :
http://www.professionalsecurity.co.uk/newsdetails.aspx?NewsArticleID=8192&imgID=1

New Vulnerabilities Tested in SecureScout

- **16791 Windows Kernel Vulnerability (MS07-066/943078) (Remote File Checking)**

An elevation of privilege vulnerability exists in the way that the Windows kernel processes certain access requests. This vulnerability could allow an attacker to run code and to take complete control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

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

References:

* MS: MS07-066
http://www.microsoft.com/technet/security/bulletin/ms07-066.mspx

CVE Reference: CVE-2007-5350

- **16789 SMBv2 Signing Vulnerability (MS07-063/942624) (Remote File Checking)**

A remote code execution vulnerability exists in the SMBv2 protocol that could allow a remote anonymous attacker to run code with the privileges of the logged-on user.

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

References:

* MS: MS07-063
http://www.microsoft.com/technet/security/bulletin/ms07-063.mspx

CVE Reference: CVE-2007-5351

❖ 16788 DHTML Object Memory Corruption Vulnerability (MS07-069/942615) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer displays a Web page that contains certain unexpected method calls to HTML objects. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code if a user visited a specially crafted Web site. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

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

References:

* MS: MS07-069
http://www.microsoft.com/technet/security/bulletin/ms07-069.mspx

CVE Reference: CVE-2007-5347

❖ 16786 Uninitialized Memory Corruption Vulnerability (CVE-2007-3903) (MS07-069/942615) (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 gain the same user rights as the logged on user.

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

References:

* MS: MS07-069
http://www.microsoft.com/technet/security/bulletin/ms07-069.mspx

CVE Reference: CVE-2007-3903

❖ 16785 Uninitialized Memory Corruption Vulnerability (CVE-2007-3902) (MS07-069/942615) (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 gain the same user rights as

the logged on user.

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

References:

* MS: MS07-069
http://www.microsoft.com/technet/security/bulletin/ms07-069.mspx

CVE Reference: CVE-2007-3902

❖ 17670 ProFTPD ASCII File Translation Off-By-One Vulnerability

ProFTPD is an FTP server available for many Unix platforms.

Phantasmal Phantasmagoria has reported a vulnerability in ProFTPD, which potentially can be exploited by malicious users to compromise a vulnerable system.

The vulnerability is caused due to two off-by-one errors in the "_xlate_ascii_write()" function. These can eg. be exploited by uploading and then retrieving ("RETR") a specially crafted file.

Successful exploitation may allow execution of arbitrary code with the privileges of ProFTPD.

The vulnerability is reported in versions prior to 1.2.10.

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

References:

* BUGTRAQ: 20040302 The Cult of a Cardinal Number
http://marc.theaimsgroup.com/?l=bugtraq&m=107824679817240&w=2
* XF: proftpd-offbyone-bo(15387)
http://xforce.iss.net/xforce/xfdb/15387
* BID: 9782
http://www.securityfocus.com/bid/9782

CVE Reference: CVE-2004-0346

❖ 16784 Windows Media Format Remote Code Execution Vulnerability Parsing ASF (MS07-068/941569/944275) (Remote File Checking)

A remote code execution vulnerability exists in Windows Media Format Runtime due to the way it handles Advanced Systems Format (ASF) files. In client applications, such as Windows Media Player, an attacker could exploit the vulnerability by constructing specially crafted Windows Media Format Runtime content that could potentially allow remote code execution if a user visits a specially crafted Web site or opens an e-mail message with specially crafted content. In server applications, such as Windows Media Services, an attacker could exploit the vulnerability by constructing specially crafted Windows Media Format Runtime content that could potentially allow remote code execution if the server processes the specially crafted content. In client and

server applications, 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:

* MS: MS07-068
http://www.microsoft.com/technet/security/bulletin/ms07-068.mspx

CVE Reference: CVE-2007-0064

❖ 16783 Microsoft DirectX Code Execution Vulnerability Parsing WAV and AVI Files (MS07-064/941568) (Remote File Checking)

A remote code execution vulnerability exists in the way DirectX handles WAV and AVI format files. This vulnerability could allow code execution if a user visits a specially crafted Web site or opens an e-mail message with specially crafted content. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS07-064
http://www.microsoft.com/technet/security/bulletin/MS07-064.mspx
* FRSIRT: ADV-2007-4180
http://www.frsirt.com/english/advisories/2007/4180
* SECUNIA: 28010
http://secunia.com/advisories/28010

CVE Reference: CVE-2007-3895

❖ 16782 Microsoft DirectX Code Execution Vulnerability Parsing SAMI Files (MS07-064/941568) (Remote File Checking)

A remote code execution vulnerability exists in the way DirectX handles supported format files. This vulnerability could allow code execution if a user opened a specially crafted file. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS07-064
http://www.microsoft.com/technet/security/bulletin/MS07-064.mspx
* FRSIRT: ADV-2007-4180
http://www.frsirt.com/english/advisories/2007/4180
* SECUNIA: 28010
http://secunia.com/advisories/28010
* XF: ms-directshow-sami-code-execution(38721)
http://xforce.iss.net/xforce/xfdb/38721

CVE Reference: CVE-2007-3901

❖ **16787 Uninitialized Memory Corruption Vulnerability (CVE-2007-5344) (MS07-069/942615) (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 gain the same user rights as the logged on user.

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

References:

* MS: MS07-069
http://www.microsoft.com/technet/security/bulletin/ms07-069.mspx

CVE Reference: CVE-2007-5344

New Vulnerabilities found this Week

Microsoft Patch Tuesday
"Code execution; Privileges escalation"

This week Microsoft released patches for the following Vulnerabilities:

* Microsoft DirectX Code Execution Vulnerability Parsing SAMI Files (MS07-064/941568)
* Microsoft DirectX Code Execution Vulnerability Parsing WAV and AVI Files (MS07-064/941568)
* Windows Media Format Remote Code Execution Vulnerability Parsing ASF (MS07-068/941569/944275)
* Uninitialized Memory Corruption Vulnerability (CVE-2007-3902) (MS07-069/942615)
* Uninitialized Memory Corruption Vulnerability (CVE-2007-3903) (MS07-069/942615)
* Uninitialized Memory Corruption Vulnerability (CVE-2007-5344) (MS07-069/942615)
* DHTML Object Memory Corruption Vulnerability (MS07-069/942615)
* SMBv2 Signing Vulnerability (MS07-063/942624)
* Windows Kernel Vulnerability (MS07-066/943078)

* ProFTPD ASCII File Translation Off-By-One Vulnerability
* Message Queuing Service Remote Code Execution Vulnerability (MS07-065/937894)
* Macrovision Driver Vulnerability (MS07-067/944653)

References:
http://www.microsoft.com/technet/security/bulletin/MS07-064.mspx
http://www.microsoft.com/technet/security/Bulletin/MS07-068.mspx
http://www.microsoft.com/technet/security/bulletin/ms07-069.mspx
http://www.microsoft.com/technet/security/bulletin/ms07-063.mspx
http://www.microsoft.com/technet/security/bulletin/ms07-065.mspx
http://www.microsoft.com/technet/security/bulletin/MS07-066.mspx
http://www.microsoft.com/technet/security/bulletin/MS07-067.mspx

Samba "send_mailslot()" Buffer Overflow Vulnerability
"Execution of arbitrary code"

Secunia Research has discovered a vulnerability in Samba, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the "send_mailslot()" function. This can be exploited to cause a stack-based buffer overflow with zero bytes via a specially crafted "SAMLOGON" domain logon packet containing a username string placed at an odd offset followed by an overly long GETDC string.

Successful exploitation allows execution of arbitrary code, but requires that the "domain logons" option is enabled.

The vulnerability is confirmed in version 3.0.27a. Prior versions may also be affected.

References:
http://secunia.com/secunia_research/2007-99/
http://us3.samba.org/samba/security/CVE-2007-6015.html

Linux Kernel "mmap_min_addr" Security Bypass
"Bypass security restrictions"

A security issue has been reported in the Linux Kernel, which can be exploited by malicious, local users to bypass certain security restrictions.

The security issue is caused due to the improper enforcing of the "mmap_min_addr" limit. This can be exploited to allocate pages lower than "mmap_min_addr" by expanding the stack or via "do_brk()" in specially crafted binaries.

The security issue affects all 2.6.23 versions.

References:
http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.24-rc5

Intuit Products AnswerWorks ActiveX Control Buffer Overflow
"Compromise a user's system"

Parvez Anwar has discovered a vulnerability in various Intuit products, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the third-party AnswerWorks ActiveX control.

The vulnerability is confirmed in TurboTax Basic 2005. Please see the vendor's advisory for a list of affected products and versions.

References:
http://www.intuit.com/support/security/

Sun StarOffice/StarSuite Database Document Processing Arbitrary Java Method Execution
"Compromise a user's system"

Sun has acknowledged a vulnerability in Sun StarOffice and StarSuite, which can be exploited by malicious people to compromise a user's system.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-103141-1

Mac OS X "cs_validate_page()" Local Denial of Service
"Denial of Service"

mu-b has reported a vulnerability in Mac OS X, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the handling of return values of "hashes()" in the "cs_validate_page()" function when processing signed Mach-O binaries and can be exploited to cause a system panic.

The vulnerability is reported in Mac OS X 10.5.1. Other versions may also be affected.

References:
http://www.digit-labs.org/files/exploits/xnu-superblob-dos.c

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