netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2007 Issue # 6

February 9, 2007

Table of Contents

Product Focus

Apache Chunked Vulnerability Scanner – The Apache Chunked 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 Apache Chunked Encoding buffer overflow.

netVigilance free Single Scanners now support Windows XP Sp2. For a full list and download, go to http://www.netvigilance.com/singlescanners

netvigilance announces support for Delta Reports in SecureScout SP.

This Week in Review

Root servers under attack. ID theft and corporate espionage big on RSA. U.S. cybersecurity chief speaks of National Infrastructure Protection Plan. Corporations need to start looking at security for smartphones and PDA's.

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

- **Hackers Launch Massive Attack on Internet DNS**

Hackers on Tuesday attacked at least three of the root servers that maintain the Internet's domain name system. However, the 12-hour-long attacks were largely

unsuccessful, as most Internet users didn't notice any impact. The system's resilience is largely due to robust protection and a high degree of redundancy built into it. Hackers on Tuesday launched a denial-of-service (DoS) attack against at least three of the 13 root servers that maintain the Internet.

The attacks, which lasted for 12 hours, reportedly targeted the server that maintains the dot-org suffix, and the servers at the Department of Defense and the Internet Corporation for Assigned Names and Numbers.

e-Commerce Times

Full Story :
http://www.ecommercetimes.com/story/business/55626.html

❖ RSA Conference focuses on Identity theft and corporate espionage

The topic of data protection stole the show at the RSA Conference on computer security here this week. Identity theft and corporate espionage were dominant themes among the 15,000 attendees.And with good reason. Data are the new currency of the Internet age for legitimate and illegitimate businesses, says Howard Schmidt, former chief information security officer of eBay who now is a consultant. Data have never been shared as quickly, and in such vast amounts.

But as millions of Americans use personal data to shop and bank online, and as more companies store data electronically, they remain targets for online fraudsters, Schmidt and others said.

Microsoft Chairman Bill Gates, security experts, politicians and other analysts offered their takes on the problems, and suggestions to fix them:"The most dangerous breach."

Osnn.net

Full Story :
http://www.osnn.net/comments.php?shownews=13678

❖ New cybersecurity chief lays out guidance

Garcia's first RSA address outlines two priorities for 2007
U.S. companies and the federal government need to step up and fix the problems in their computer networks, the nation's new cybersecurity czar told attendees during his first-ever address at RSA Conference here in San Francisco on Thursday.

Within the next 10 years, the majority of the world's communication needs will probably be handled by the Internet, said Gregory Garcia, the assistant secretary for cybersecurity and telecommunications at the Department of Homeland Security (DHS). "This proliferation of applications and devices within the converged network is going to create a breeding ground for security problems," he said. "Our networks and our systems are vulnerable and they are exposed."

Garcia outlined two priorities for the year ahead. First, his office is working with federal agencies to adopt common security policies and practices. Second, he plans to work

with the private sector to push forward a process called the National Infrastructure Protection Plan. This effort is intended to evaluate computer security risks on an industry-by-industry basis and outline the steps that need to be taken to address them.

The broad strokes of this plan were outlined last June, and the DHS is now working with industry to flesh out sector-specific plans, Garcia said.

Computerworld

Full Story :
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9010939&taxonomyId=17&intsrc=kc_feat

- **Next Wave in Security: Protecting Smart Phones, PDAs**

With the number of employees using smart phones and other mobile devices, corporations must start to focus their security on more than just their network perimeter, according to security analysts and specialists attending the RSA Conference here. Research done by the Business Forum Management Program in 2006 found that roughly 49 percent of the 680 executives surveyed are "mobile" or "very mobile," and about 80 percent plan to increase the number of mobile devices used in the next few years.

And even though a quarter of the respondents reported having critical data stored on mobile devices, 40 percent said they have no security and compliance measures in place to protect data on those devices. In addition, just 17.2 percent said they are very concerned about a breach in their company's mobile communications—almost the same amount that reported being unconcerned.

eweek

Full Story :
http://www.eweek.com/article2/0,1895,2093092,00.asp

New Vulnerabilities Tested in SecureScout

- **12149 PostgreSQL Denial of Service and Information Disclosure Vulnerabilities**

Some vulnerabilities have been reported in PostgreSQL, which can be exploited by malicious users to gain knowledge of potentially sensitive information and cause a DoS (Denial of Service).

An unspecified error can be used to suppress certain checks, which ensure that SQL functions return the correct data type. This can be exploited to crash the database backend or disclose potentially sensitive information.

PostgreSQL versions prior to 8.0.11, and 8.1.7, 8.2.2 are vulnerable to these issues.

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

References:

Original advisory:
http://www.postgresql.org/support/security

Other references:
* UBUNTU:USN-417-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-417-1
* FRSIRT:ADV-2007-0478
* URL:http://www.frsirt.com/english/advisories/2007/0478
* SECUNIA:24033
* URL:http://secunia.com/advisories/24033

Home page:
http://www.postgresql.org/

CVE Reference: CVE-2007-0555

❖ 12150 PostgreSQL changing data type of a table column, Denial of Service and Information Disclosure Vulnerabilities

Some vulnerabilities have been reported in PostgreSQL, which can be exploited by malicious users to gain knowledge of potentially sensitive information and cause a DoS (Denial of Service).

An unspecified error when changing the data type of a table column can be exploited to crash the database backend or disclose potentially sensitive information.

PostgreSQL versions prior to 7.3.13, 7.4.16, 8.0.11, and 8.1.7, 8.2.2 are vulnerable to these issues.

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

References:

Original advisory:
http://www.postgresql.org/support/security

Other references:
* UBUNTU:USN-417-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-417-1
* FRSIRT:ADV-2007-0478
* URL:http://www.frsirt.com/english/advisories/2007/0478
* SECUNIA:24033
* URL:http://secunia.com/advisories/24033

Home page:
http://www.postgresql.org/

CVE Reference: CVE-2007-0556

❖ 14050 Samba Denial of Service Vulnerability

A vulnerability has been reported in Samba, which can be exploited by malicious users to cause a DoS (Denial of Service).

Under certain conditions, smbd fails to remove requests from the deferred file open queue. This can be exploited to cause a DoS due to heavy resource usage by triggering an infinite loop when renaming a file under special circumstances.

The security issue has been fixed in version 3.0.24.

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

References:

Initial advisory:
* BUGTRAQ:20070205 [SAMBA-SECURITY] CVE-2007-0452: Potential DoS against smbd in Samba 3.0.6 - 3.0.23d
http://www.securityfocus.com/archive/1/archive/1/459167/100/0/threaded

Other references:
http://secunia.com/advisories/24046/

Product Page:
http://www.samba.org

CVE Reference: CVE-2007-0452

❖ 14051 Samba Format String Vulnerability

A vulnerability has been reported in Samba, which can be exploited by malicious users to compromise a vulnerable system.

Samba uses filenames as format string parameter in a call to "sprintf()" when setting Windows NT Access Control Lists using the afsacl.so VFS plugin. This can potentially be exploited to execute arbitrary code.

Successful exploitation requires that an AFS file system is shared to CIFS clients using the afsacl.so VFS module and that the attacker has write access to the share.

The security issue has been fixed in version 3.0.24.

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

References:

Initial advisory:
* BUGTRAQ:20070205 [SAMBA-SECURITY] CVE-2007-0454: Format string bug in afsacl.so VFS plugin
http://www.securityfocus.com/archive/1/archive/1/459179/100/0/threaded

Other references:
* BID:22403
http://www.securityfocus.com/bid/22403
* SECUNIA:

http://secunia.com/advisories/24046/

Product Page:
http://www.samba.org

CVE Reference: CVE-2007-0454

❖ 14053 Samba Multiple Share Connection Requests Denial of Service

A vulnerability has been reported in Samba, which can be exploited by malicious users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error when handling a lot of share connection requests. This can be exploited to cause smbd to exhaust memory resources via a large number of share connections.

The vulnerability has been reported in versions 3.0.1 through 3.0.22.

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

References:

CVE Reference: CVE-2006-3403

❖ 16413 Vulnerability in Microsoft Office Could Allow Remote Code Execution (932553) (Remote File Checking)

A vulnerability has been reported in Microsoft Office, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error when handling strings and can be exploited to cause a memory corruption.

Successful exploitation allows execution of arbitrary code.

NOTE: According to Microsoft, the vulnerability is currently being actively exploited via Excel, but other Office applications may also be affected.

This Testcase tests only Microsoft Office Excel component.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/advisory/932553.mspx

Other references:
* MISC: http://vil.nai.com/vil/content/v_141393.htm

* MISC: http://www.avertlabs.com/research/blog/?p=191
* FRSIRT:ADV-2007-0463
* URL:http://www.frsirt.com/english/advisories/2007/0463
* SECTRACK:1017584
* URL:http://securitytracker.com/id?1017584

CVE Reference: CVE-2007-0671

❖ 16414 WinRAR UnRAR Password Prompt Buffer Overflow Vulnerability (Remote File Checking)

A vulnerability has been reported in RARLabs UnRAR, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when processing password-protected archives using the UnRAR command line utility. This can be exploited to cause a stack-based buffer overflow via a specially crafted password-protected archive.

Successful exploitation requires that the user is e.g. tricked into opening a password-protected archive and respond to the password prompt.

The vulnerability is reported in version 3.60 for Linux and 3.61 for Windows. Other versions may also be affected.

The vendor has issued version 3.70 beta release to fix the issue.

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

References:

Original advisory:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=472

Other references:
http://secunia.com/advisories/24077/

Product Homepage:
http://www.rarlabs.com/

CVE Reference:

❖ 16415 WinRAR Format String Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in WinRAR, which can be exploited by malicious people to compromise a user's system.

A format string error exists when displaying a diagnostic error message that informs the user of an invalid filename in an UUE/XXE encoded file. This can be exploited to execute arbitrary code when a malicious UUE/XXE file is decoded.

WinRAR version 3.51 has been released to address this specific issue.

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

References:

Original advisory:
http://secunia.com/secunia_research/2005-53/advisory/

Other references:
* CONFIRM:http://www.rarlabs.com/rarnew.htm
* BID:15062
* URL:http://www.securityfocus.com/bid/15062
* SECUNIA:16973
* URL:http://secunia.com/advisories/16973/

Product Homepage:
http://www.rarlabs.com/

CVE Reference: CVE-2005-3262

❖ 16416 WinRAR Buffer Overflow Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in WinRAR, which can be exploited by malicious people to compromise a user's system.

A boundary error in UNACEV2.DLL can be exploited to cause a stack-based buffer overflow. This allows arbitrary code execution when a malicious ACE archive containing a file with an overly long file name is extracted.

WinRAR version 3.51 has been released to address this specific issue.

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

References:

Original advisory:
http://secunia.com/secunia_research/2005-53/advisory/

Other references:
* FULLDISC:20051011 Secunia Research: WinRAR Format String and Buffer Overflow Vulnerabilities
* URL:http://archives.neohapsis.com/archives/fulldisclosure/2005-10/0266.html
* CONFIRM: http://www.rarlabs.com/rarnew.htm
* BID:15062
* URL:http://www.securityfocus.com/bid/15062
* OSVDB:19915
* URL:http://www.osvdb.org/19915
* SECUNIA:16973
* URL:http://secunia.com/advisories/16973/

Product Homepage:
http://www.rarlabs.com/

CVE Reference: CVE-2005-3263

❖ **16417 WinRAR LHA Archive Processing Buffer Overflow (Remote File Checking)**

Ryan Smith has reported a vulnerability in WinRAR, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to boundary errors in lzh.fmt within the processing of LHA archives. This can be exploited to cause a stack-based buffer overflow when a specially crafted file with an overly long filename is opened.

Successful exploitation allows execution of arbitrary code with the user's privileges.

The vulnerability has been reported in versions 3.00 through 3.60 beta 6.
The vulnerability has been fixed in version 3.60 beta 7.

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

References:

Original advisory:
http://hustlelabs.com/advisories/04072006_rarlabs.pdf

Other references:
* CONFIRM: http://www.rarlabs.com/rarnew.htm
* FRSIRT:ADV-2006-2867
* URL:http://www.frsirt.com/english/advisories/2006/2867
* SECUNIA:21080
* URL:http://secunia.com/advisories/21080
* XF:winrar-lha-bo(27815)
* URL:http://xforce.iss.net/xforce/xfdb/27815

Product Homepage:
http://www.rarlabs.com/

CVE Reference: CVE-2006-3845

New Vulnerabilities found this Week

Microsoft Office Unspecified String Handling Vulnerability
"Execution of arbitrary code"

A vulnerability has been reported in Microsoft Office, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an unspecified error when handling strings and can be exploited to cause a memory corruption.

Successful exploitation allows execution of arbitrary code.

NOTE: According to Microsoft, the vulnerability is currently being actively exploited via Excel, but other Office applications may also be affected.

References:
http://www.microsoft.com/technet/security/advisory/932553.mspx
http://www.kb.cert.org/vuls/id/613740
http://descriptions.securescout.com/tc/16413

RARLabs UnRAR Password Prompt Buffer Overflow Vulnerability
"Execution of arbitrary code"

A vulnerability has been reported in RARLabs UnRAR, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error when processing password-protected archives using the UnRAR command line utility. This can be exploited to cause a stack-based buffer overflow via a specially crafted password-protected archive.

Successful exploitation requires that the user is e.g. tricked into opening a password-protected archive and respond to the password prompt.

The vulnerability is reported in version 3.60 for Linux and 3.61 for Windows. Other versions may also be affected.

References:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=472
http://descriptions.securescout.com/tc/16414

Samba Denial of Service and Format String Vulnerability
"Denial of Service; Code execution"

Some vulnerabilities have been reported in Samba, which can be exploited by malicious users to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

1) Under certain conditions, smbd fails to remove requests from the deferred file open queue. This can be exploited to cause a DoS due to heavy resource usage by triggering an infinite loop when renaming a file under special circumstances.

2) Samba uses filenames as format string parameter in a call to "sprintf()" when setting Windows NT Access Control Lists using the afsacl.so VFS plugin. This can potentially be exploited to execute arbitrary code.

Successful exploitation requires that an AFS file system is shared to CIFS clients using the afsacl.so VFS module and that the attacker has write access to the share.

References:
http://us1.samba.org/samba/security/CVE-2007-0452.html
http://us1.samba.org/samba/security/CVE-2007-0454.html
http://www.kb.cert.org/vuls/id/649732
http://descriptions.securescout.com/tc/14050
http://descriptions.securescout.com/tc/14051

Samba Winbind Library Buffer Overflow Vulnerabilities

“Execution of arbitrary code”

Two vulnerabilities have been reported in Samba, which potentially can be exploited by malicious people to compromise a vulnerable system.

The vulnerabilities are caused due to boundary errors within the "gethostbyname()" and "getipnodebyname()" functions in the "nss_winbind.so.1" library. This can be exploited to cause a buffer overflow via an overly large string passed to the NSS interface.

Successful exploitation may allow execution of arbitrary code, but requires that the winbindd daemon is running and configured to use the "nss_winbind.so.1" library.

The vulnerabilities are reported in version 3.0.21 through 3.0.23d running on Sun Solaris

References:
http://us1.samba.org/samba/security/CVE-2007-0453.html

pam_ssh "allow_blank_passphrase" Bypass Security Issue

“Bypass security restrictions”

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

The security issue is caused due to pam_ssh not properly restricting the use of private keys with a blank password, even if the "allow_blank_password" option is disabled. This can be exploited to use private keys with blank passphrases by entering a random, non-blank passphrase when prompted.

The security issue is reported in version 1.91.

References:
http://sourceforge.net/project/shownotes.php?release_id=484376

PostgreSQL Denial of Service and Information Disclosure

“Denial of Service; Information Disclosure”

Some vulnerabilities have been reported in PostgreSQL, which can be exploited by malicious users to gain knowledge of potentially sensitive information and cause a DoS (Denial of Service).

1) An unspecified error can be used to suppress certain checks, which ensure that SQL functions return the correct data type. This can be exploited to crash the database backend or disclose potentially sensitive information.

2) An unspecified error when changing the data type of a table column can be exploited to crash the database backend or disclose potentially sensitive information.

Vulnerability #1 is reported in versions 8.0, 8.1, and 8.2. Vulnerability #2 is reported in 8.0, 8.1, 8.2, 7.3 and 7.4.

References:
http://www.postgresql.org/support/security
http://descriptions.securescout.com/tc/12149

Bugzilla Cross-Site Scripting Vulnerability
"Cross-Site Scripting"

A vulnerability has been reported in Bugzilla, which can be exploited by malicious users to conduct cross-site scripting attacks.

Input passed to certain fields (e.g. the realname field) is not properly sanitized before being used to generate Atom feeds. This can be exploited to execute arbitrary HTML and script code in a user's atom feed reader in context of an affected site.

The vulnerability is reported in versions prior to 2.20.4, 2.22.2, and 2.23.4.

References:
http://www.bugzilla.org/security/2.20.3/

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