netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 27

July 7, 2006

Table of Contents

Product Focus

Mydoom Worm Scanner – The S4 MyDoom Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by the MyDoom email virus or its variants.

New SecureScout SP Feature this week : you can now create and delete SP users from the commandline via new parameters to CLI.exe

This Week in Review

Security breaches continually rising as companies still leave backdoors open. New approach to protect against hackers. Maybe the future holds software built to be stronger with fewer vulnerabilities.

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

- **Businesses Security Breaches Rising**

More than 84 percent of North American enterprises have had their security breached within the past year, according to a recent survey.

Breaches grew by 17 percent over the past three years and the number of incidents continues to rise, according to results announced Wednesday by CA, formerly Computer Associates.

Security incidents caused 54 percent of organizations to lose productivity, according to the survey, conducted from January through May 2006, by The Strategic Counsel. Twenty-five percent said they were publicly embarrassed or suffered a loss of confidence and damage to reputation; and 20 percent reported loss of revenue, customers or other tangible assets. Thirty-eight percent of the organizations reporting security incidents said the breaches were internal.

TechWeb Technology News

Full Story :
http://www.techweb.com/showArticle.jhtml?articleID=190300376&cid=RSSfeed_TechWeb

❖ DOE's Federated Model aims to identify security threats

Argonne National Laboratory, a division of the Department of Energy (DOE) operated out of the University of Chicago, is spearheading an effort to collect information about cyber security events that is beginning to gain steam.

Called The Federated Model, this information-sharing initiative among government, universities, and research labs began last September and currently has about half a dozen active members, says Scott Pinkerton, manager of network services for the lab in DuPage County, Ill.

The initiative is open to any organization wanting to share details, or even just view information, regarding attempts by different IP addresses to access networks and how organizations have responded to these attempts, in an effort to spot patterns of malicious behavior and proactively block security threats, says Pinkerton.

Network World

Full Story :

http://www.computerworld.com.au/index.php/id;384626279;fp;16;fpid;0

❖ Corporates Still Leave Security Back Doors Open

End point security which is a key component in the information security defences of organisations, is being totally overlooked by a significant number of organisations, according to a survey released today by Secure Computing Corporation (NASDAQ: SCUR). A fifth of organisations do not have any form of end point security which means that their corporate networks and data are potentially exposed to hackers and criminals who can access sensitive information from unprotected access points.

In addition 49% of organisations do not even use desktop firewalls for end point security, this is the most basic and fundamental level of security that should be deployed to prevent unauthorised access to sensitive information.

Protecting the operating system by ensuring it has the latest available patches installed is a further area that needs improvement with over a third (37%) of organisations not keeping their operating systems up-to-date.

ITSecurity

Full Story :
http://www.itsecurity.com/security.htm?s=18136&sid=39ea64b4c5e5aba16b73095c881317ed

❖ Method to Better Predict Software Vulnerabilities

Vulnerability defects in software that can allow hackers to bypass security measures have emerged as a significant threat in a society that increasingly relies on computer systems and the Internet for commerce and other uses.

Researchers at Colorado State University have developed a model to predict with much greater accuracy the number and severity of vulnerabilities that will likely surface in operating systems and in major software applications in the near future. The research is lead by Yashwant K. Malaiya, professor in the Department of Computer Science in Colorado State's College of Natural Sciences. Malaiya is assisted by doctoral student Omar Alhazmi.

In 2005 alone, 5,198 newly discovered vulnerabilities were reported by the U.S. Department of Homeland Security's Computer Emergency Readiness Team, or CERT. Such vulnerabilities can be exploited by hackers if they are discovered and not quickly fixed through patches - updates to fix security problems.

Softpedia news

Full Story :
http://news.softpedia.com/news/Method-to-Better-Predict-Software-Vulnerabilities-28574.shtml

New Vulnerabilities Tested in SecureScout

❖ 12116 PostgreSQL Database is not password protected

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

A vulnerability exists in the default installation of the PostgreSQL database which creates a default user/password pairing allowed by leaving "method" account in the conf file set to its default password "trust".

This default configuration can easily be discovered and accessed remotely by an attacker because of the existence of a default database by the name of template1. Upon discovery this can exploited to the total compromise of the target system.

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

References:

http://osvdb.org/displayvuln.php?osvdb_id=382

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

CVE Reference:

❖ 12117 PostgreSQL Database Version Disclosure

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

Identifying the PostgreSQL Database version could be useful in further attacks against the target.

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

References:

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

CVE Reference:

❖ 12118 PostgreSQL Multibyte Character Encoding SQL Injection Vulnerabilities

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

PostgreSQL is prone to SQL-injection vulnerabilities. These issues are due to a potential mismatch of multibyte character conversions between PostgreSQL servers and client applications.

A successful exploit could allow an attacker to execute arbitrary SQL statements on affected servers. This may allow the attacker to compromise the targeted computer, access or modify data, or exploit other latent vulnerabilities.

PostgreSQL versions prior to 7.3.15, 7.4.13, 8.0.8, and 8.1.4 are vulnerable to these issues.

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

References:

http://www.securityfocus.com/archive/1/435038
http://www.postgresql.org/docs/techdocs.50
http://archives.postgresql.org/pgsql-announce/2006-05/msg00010.php
http://rhn.redhat.com/errata/RHSA-2006-0526.html
http://www.postgresql.org/docs/8.1/static/release-8-0-8.html
http://www.postgresql.org/docs/8.1/static/release-7-4-13.html
http://www.postgresql.org/docs/8.1/static/release-7-3-15.html
http://www.postgresql.org/
http://www.postgresql.org/docs/8.1/static/release.html
http://support.avaya.com/elmodocs2/security/ASA-2006-113.htm

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

CVE Reference: CVE-2006-2313
CVE-2006-2314

❖ 12119 PostgreSQL path_add() Buffer Overrun Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

PostgreSQL is prone to a buffer overflow in the path_add() function. The vulnerability is due to insufficient bounds checking of user-supplied data.

Successful exploitation will enable an attacker to execute code in the content of the database server process. A denial of service may also be the result of exploitation attempts.

PostgreSQL version 7.2.3 and earlier are vulnerable to this issue.

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

References:

* MISC: http://archives.postgresql.org/pgsql-hackers/2002-08/msg02047.php
* MISC: http://archives.postgresql.org/pgsql-hackers/2002-08/msg02081.php
* DEBIAN:DSA-165
* URL:http://www.debian.org/security/2002/dsa-165
* CONECTIVA:CLA-2002:524
* URL:http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000524

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

CVE Reference: CVE-2002-1401

❖ 12120 PostgreSQL path_encode() Buffer Overflow Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

A buffer overrun exists in the 'path_encode()' function which may allow an attacker to overwrite sensitive locations in memory.

By exploiting this issue to overwrite an instruction pointer in the program, it may be possible for a remote attacker to execute arbitrary commands. All commands will be executed with the privileges of the database process.

PostgreSQL version 7.2.3 and earlier are vulnerable to this issue.

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

References:

* MISC: http://archives.postgresql.org/pgsql-hackers/2002-08/msg02047.php
* MISC: http://archives.postgresql.org/pgsql-hackers/2002-08/msg02081.php
* DEBIAN:DSA-165
* URL:http://www.debian.org/security/2002/dsa-165
* CONECTIVA:CLA-2002:524
* URL:http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000524

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

CVE Reference: CVE-2002-1401

❖ 12121 PostgreSQL To_Ascii() Buffer Overflow Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

PostgreSQL is reported prone to a buffer overflow vulnerability, which presents itself in the PostgreSQL to_ascii() function. The to_ascii() function is normally used to convert text from multibyte encoding format to ASCII.

It has been conjectured that excessive data passed to the to_ascii() function may overrun the bounds of an insufficient buffer reserved in heap based memory. This may result in the corruption of heap based memory management structures that are adjacent to the affected buffer. Although unconfirmed, it is currently believed that under the correct circumstances an attacker may leverage this condition to execute arbitrary instructions in the context of the affected service.

Other ADT (abstract data type) to_ascii_xxx() conversion functions are similarly affected.

PostgreSQL version 7.2.x, and 7.3.x before 7.3.4 are vulnerable to this issue.

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

References:

* CONECTIVA:CLSA-2003:772
* URL:http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000772
* CONFIRM: http://developer.postgresql.org/cvsweb.cgi/pgsql-server/src/backend/utils/adt/ascii.c
* DEBIAN:DSA-397
* URL:http://www.debian.org/security/2003/dsa-397
* REDHAT:RHSA-2003:313
* URL:http://www.redhat.com/support/errata/RHSA-2003-313.html
* REDHAT:RHSA-2003:314
* URL:http://www.redhat.com/support/errata/RHSA-2003-314.html
* CONECTIVA:CLA-2003:784
* URL:http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000784
* BID:8741
* URL:http://www.securityfocus.com/bid/8741

Home page:

http://www.postgresql.org/

CVE Reference: CVE-2003-0901

❖ 12122 PostgreSQL Aggregate Function EXECUTE Restriction Bypass

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

PostgreSQL 8.0.0 and earlier allows local users to bypass the EXECUTE permission check for functions by using the CREATE AGGREGATE command.

An attacker may leverage this issue to execute arbitrary code with the privileges of the vulnerable database process and to execute functions without requiring permission. Other attacks are also possible.

PostgreSQL version 8.0.0 and earlier are vulnerable to this issue.

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

References:

* MLIST:[pgsql-hackers] 20050127 Permissions on aggregate component functions
* URL:http://archives.postgresql.org/pgsql-hackers/2005-01/msg00922.php
* MANDRAKE:MDKSA-2005:040
* URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:040
* REDHAT:RHSA-2005:138
* URL:http://www.redhat.com/support/errata/RHSA-2005-138.html
* BUGTRAQ:20050210 [USN-79-1] PostgreSQL vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=110806034116082&w=2
* SUSE:SUSE-SA:2005:036
* URL:http://www.novell.com/linux/security/advisories/2005_36_sudo.html
* SECUNIA:12948
* URL:http://secunia.com/advisories/12948
* XF:postgresql-security-bypass(19184)
* URL:http://xforce.iss.net/xforce/xfdb/19184

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

CVE Reference: CVE-2005-0244

❖ 12123 PostgreSQL refcursor function arbitrary code execution

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

A Buffer overflow in gram.y for PostgreSQL 8.0.0 and earlier may allow attackers to execute arbitrary code via a large number of arguments to a refcursor function (gram.y), which leads to a heap-based buffer overflow, a different vulnerability than CVE-2005-0247.

An attacker may leverage this issue to execute arbitrary code with the privileges of the vulnerable database process and to execute functions without requiring permission. Other attacks are also possible.

PostgreSQL version 8.0.0 and earlier are vulnerable to this issue.

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

References:

* MLIST:[pgsql-patches] 20050120 Re: WIP: pl/pgsql cleanup
* URL:http://archives.postgresql.org/pgsql-patches/2005-01/msg00216.php
* MLIST:[pgsql-committers] 20050121 pgsql: Prevent overrunning a heap-allocated buffer is more than 1024
* URL:http://archives.postgresql.org/pgsql-committers/2005-01/msg00298.php
* MLIST:[pgsql-committers] 20050207 pgsql: Prevent 4 more buffer overruns in the PL/PgSQL parser.
* URL:http://archives.postgresql.org/pgsql-committers/2005-02/msg00049.php
* DEBIAN:DSA-683
* URL:http://www.debian.org/security/2005/dsa-683
* MANDRAKE:MDKSA-2005:040
* URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:040
* REDHAT:RHSA-2005:138
* URL:http://www.redhat.com/support/errata/RHSA-2005-138.html
* REDHAT:RHSA-2005:150
* URL:http://www.redhat.com/support/errata/RHSA-2005-150.html
* BUGTRAQ:20050210 [USN-79-1] PostgreSQL vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=110806034116082&w=2
* SUSE:SUSE-SA:2005:036
* URL:http://www.novell.com/linux/security/advisories/2005_36_sudo.html
* SECUNIA:12948
* URL:http://secunia.com/advisories/12948
* XF:postgresql-cursor-bo(19188)
* URL:http://xforce.iss.net/xforce/xfdb/19188

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

CVE Reference: CVE-2005-0245

❖ 12124 PostgreSQL intagg contrib module denial of service Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

The intagg contrib module for PostgreSQL 8.0.0 and earlier allows attackers to cause a denial of service (crash) via crafted arrays.

PostgreSQL version 8.0.0 and earlier are vulnerable to this issue.

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

References:

* MLIST:[pgsql-committers] 20050127 pgsql: Fix security and 64-bit issues in contrib/intagg.
* URL:http://archives.postgresql.org/pgsql-committers/2005-01/msg00401.php
* MANDRAKE:MDKSA-2005:040
* URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:040
* REDHAT:RHSA-2005:138
* URL:http://www.redhat.com/support/errata/RHSA-2005-138.html
* BUGTRAQ:20050210 [USN-79-1] PostgreSQL vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=110806034116082&w=2
* SUSE:SUSE-SA:2005:036
* URL:http://www.novell.com/linux/security/advisories/2005_36_sudo.html
* SECUNIA:12948
* URL:http://secunia.com/advisories/12948
* XF:postgresql-contribintagg-dos(19185)
* URL:http://xforce.iss.net/xforce/xfdb/19185

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

CVE Reference: CVE-2005-0246

❖ 12125 PostgreSQL Multiple buffer overflows in gram.y arbitrary code execution Vulnerability

PostgreSQL Database server is a very popular database server which sees widespread use throughout the world.

Multiple buffer overflows in gram.y for PostgreSQL 8.0.1 and earlier may allow attackers to execute arbitrary code via (1) a large number of variables in a SQL statement being handled by the read_sql_construct function, (2) a large number of INTO variables in a SELECT statement being handled by the make_select_stmt function, (3) a large number of arbitrary variables in a SELECT statement being handled by the make_select_stmt function, and (4) a large number of INTO variables in a FETCH statement being handled by the make_fetch_stmt function, a different set of vulnerabilities than CVE-2005-0245.

An attacker may leverage these issues to execute arbitrary code with the privileges of the vulnerable database process and to execute functions without requiring permission. Other attacks are also possible.

PostgreSQL version 8.0.1 and earlier are vulnerable to this issue.

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

References:

* MLIST:[pgsql-committers] 20050207 pgsql: Prevent 4 more buffer overruns in the PL/PgSQL parser.
* URL:http://archives.postgresql.org/pgsql-committers/2005-02/msg00049.php
* DEBIAN:DSA-683
* URL:http://www.debian.org/security/2005/dsa-683
* GENTOO:GLSA-200502-19

* URL:http://www.gentoo.org/security/en/glsa/glsa-200502-19.xml
* MANDRAKE:MDKSA-2005:040
* URL:http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:040
* REDHAT:RHSA-2005:138
* URL:http://www.redhat.com/support/errata/RHSA-2005-138.html
* REDHAT:RHSA-2005:150
* URL:http://www.redhat.com/support/errata/RHSA-2005-150.html
* SUSE:SUSE-SA:2005:027
* URL:http://www.novell.com/linux/security/advisories/2005_27_postgresql.html
* BUGTRAQ:20050210 [USN-79-1] PostgreSQL vulnerabilities
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=110806034116082&w=2
* SUSE:SUSE-SA:2005:036
* URL:http://www.novell.com/linux/security/advisories/2005_36_sudo.html
* XF:postgresql-fetch-makefetchstmt-bo(19378)
* URL:http://xforce.iss.net/xforce/xfdb/19378
* XF:postgresql-makeselectstmt-arbitrary-bo(19377)
* URL:http://xforce.iss.net/xforce/xfdb/19377
* XF:postgresql-makeselectstmt-input-bo(19376)
* URL:http://xforce.iss.net/xforce/xfdb/19376
* XF:postgresql-readsqlconstruct-bo(19375)
* URL:http://xforce.iss.net/xforce/xfdb/19375

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

CVE Reference: CVE-2005-0247

New Vulnerabilities found this Week

ppp setuid Security Issue

"Perform certain actions with escalated privileges"

Marcus Meissner discovered a vulnerability in the winbind plugin of ppp, which potentially can be exploited by malicious, local users to perform certain actions with escalated privileges.

The security issue is caused due to missing checks for whether the "setuid()" call has succeeded. This can potentially be exploited to launch the winbind NTLM authentication helper with root privileges, which may allow the user to perform certain actions as the root user.

Successful exploitation allows performing certain actions with escalated privileges, but requires special PAM and ppp configurations.

This vulnerability has been reported in version 2.4.3 and 2.4.4b1. Prior versions may also be affected.

References:
http://www.ubuntu.com/usn/usn-310-1

shadow setuid Vulnerability

"Perform certain actions with escalated privileges"

Ilja van Sprundel reported a vulnerability in the passwd application of shadow, which potentially can be exploited by malicious, local users to perform certain actions with escalated privileges.

The vulnerability is due to missing checks in passwd for whether the "setuid()" call has succeeded, when started with the -f, -g, or -s option. This can potentially be exploited to launch chfn, chsh, or gpasswd with root privileges, which may allow the user to perform certain actions as the root user.

Successful exploitation allows to perform certain actions with escalated privileges, but requires that PAM is configured with a maximum number of user processes.

This vulnerability was reported in version 4.0.3 and 4.0.13. Prior versions may be also affected.

References:
http://www.ubuntu.com/usn/usn-308-1

Internet Explorer HTML Help ActiveX Control Memory Corruption

"Execution of arbitrary code"

HD Moore has discovered a vulnerability in Internet Explorer, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to an error in the HTML Help ActiveX control (hhctrl.ocx) when handling the "Image" property. This can be exploited to cause a memory corruption by setting an overly long string multiple times for the property.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been confirmed on a fully patched system running Windows XP SP2 with Internet Explorer 6.0. Other versions may also be affected.

References:
http://browserfun.blogspot.com/2006/07/mobb-2-internethhctrl-image-property.html

Sun Java System Messaging Server Arbitrary File Disclosure

"Gain knowledge of potentially sensitive information."

php0t has reported a vulnerability in Sun Java System Messaging Server / iPlanet Messaging Server, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information.

The vulnerability is caused due to the setuid program "pipe_master" reading the msg.conf configuration file using the path specified in the "CONFIGROOT" environment variable. This can be exploited via symlink attacks to disclose the first line of arbitrary files in the returned error message.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102496-1

Linux Kernel SCTP Denial of Service Vulnerability

"Denial of Service"

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

The vulnerability is caused due to an error when handling SCTP packets without a chunk. This can be exploited to crash the kernel by sending a specially crafted SCTP packet to a vulnerable system.

References:
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.16.23
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.17.3

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