ScoutNews Team **30 April 2004**
Issue #18

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Symantec excused its claim that malicious code to exploit the TPC vulnerability already existed.
Fighting the ever more intelligent and sophisticated worms is taking up more and more of our available time. For those of our readers who subscribe to SecureScout and use it on a regular basis; you will be please to see we are continuing our efforts to help out here.
Some MS patches slowed SSL functionality down.
Wireless is becoming more and more center stage.

Enjoy reading

Top Security News Stories this Week

❖ **Microsoft SSL patch creating SSLowdowns**

Some systems that use the security update, MS04-011, stop responding when they start up, prevent users from logging on to Windows, or bog down, Microsoft said in an article published Wednesday in its Knowledge Base online help database.
The security patch was released on April 13 and fixes a number of holes in Windows, including problems with Windows implementation of Secure Sockets Layer (SSL), a protocol that frequently used to secure communications between servers and clients on public networks and the Internet.
http://www.infoworld.com/article/04/04/29/HNmsftpatch_1.html
Paul Roberts

❖ **Lawmakers vow to pass new law against spyware**

U.S. lawmakers vowed today to pass legislation to stop deceptive software even though regulators advised against any new laws.
Both Republicans and Democrats on the House Energy and Commerce Committee said new laws were needed to stop the proliferation of so-called spyware, which hides in users' computers and secretly monitors their activities.
"There is no more pernicious, intrusive activity going on on the Internet today," said Rep. Joe Barton (R-Texas), chairman of the House Energy and Commerce Committee. "We really intend to do something about this."
http://www.computerworld.com/governmenttopics/government/legislation/story/0,10801

,92762,00.html?f=x10
Peter Kaplan

❖ **Hacker Hits License Plate Database**

The FBI and secretary of state police were trying to determine how a hacker tapped into as many as 200,000 temporary license plate records in an Illinois secretary of state computer database over the weekend, officials said.

Only the temporary registration permit database was compromised, not the main drivers' license system that includes Social Security numbers, secretary of state spokesman Dave Druker said Wednesday.

http://cbs2chicago.com/topstories/local_story_120165420.html
Mike Flannery

❖ **Protecting Road Warriors: Managing Security for Mobile Users (Part One)**

Managing security within the confines of an organization or enterprise is a difficult job. Worms, viruses, spam, malware, port scans and perimeter defense probes are constant threats. Servers and desktop systems require regular patching and monitoring, and IDS signatures and firewall rules are under constant review and tweaking. Thankfully, the desktops and servers sit well protected within the confines of your network. Imagine what it would be like if every user's system was located on your network perimeter and had none of the safeguards your multi-layered security systems provide.

Unfortunately, you most likely have such systems: your mobile users. Whether it's your sales force, world-traveling executives or just a user "working from home," these people are separated from all of your inner defenses and are at the mercy of their surroundings. You need a strategy to ensure their systems and their data is as safe on the road as they are in your own borders.

http://www.securityfocus.com/infocus/1777
Bob Rudis

❖ **DOD decentralizes Wi-Fi**

The Defense Department's new wireless fidelity policy seeks help from many of its agencies to ensure their employees and contractors use caution when operating wireless computer devices at military installations.

The chief information officer and DOD's Office of Networks and Information Integration (NI2) oversee and monitor the new Wi-Fi policy. But the undersecretary of Defense for Intelligence, the Chairman of the Joint Chiefs of Staff, the U.S. Strategic Command, the Defense Information Systems Agency and department staff officials all get roles in the new policy.

http://www.fcw.com/fcw/articles/2004/0426/web-wifi-04-26-04.asp
Frank Tiboni

❖ **UK, US and Canada crack down on Net scams**

The UK, US and Canada are to work even closer together in a bid to tackle international scams - many of which are peddled via the Net.

New intelligence-sharing arrangements with the Canadian Competition Bureau, the US Federal Trade Commission and the UK's Office of Fair Trading (OFT) should make it easier for law enforcers to nab villains.

http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/57506862?-2622
Tim Richardson

❖ **Symantec says it erred in judging exploit code**

Security services and A-V software maker Syamntec says it erred in concluding that code its experts found on the net was an exploit which could be used to target a flaw in the Private Communications Transport (PCT) protocol implementation of the Microsoft Secure Socket Layer library.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/57319333?-2622
Sam Verghese

❖ **Experts warn of Bluetooth security hole**

Thieves have acquired new weapons to exploit Bluetooth-enabled phones and computers to steal valuable data, experts warn.
Though Bluetooth integrates certain security measures, security expert Adam Laurie has shown reporters at the BBC how he can 'bluesnarf' into other Bluetooth-enabled devices without permission using some software and a Bluetooth-capable computer.
http://www.snpx.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/57504965?-2622
Macworld

New Vulnerabilities Tested in SecureScout

➢ **14428 W32/Netsky.s Worm (Registry Check)**

Description: This worm:
Constructs messages using its own SMTP engine
Harvests email addresses from the victim machine
Spoofs the From: address of messages
Opens a port on the victim machine (TCP 6789)
Delivers a DoS attack on certain web sites upon a specific date condition

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101156

➢ **14429 W32/Bagle.z Worm (Registry Check)**

This is a mass-mailing worm with the following characteristics:

Contains its own SMTP engine to construct outgoing messages.
Harvests email addresses from the victim machine
The From: address of messages is spoofed
Contains a remote access component (The worm sends notification via HTTP to a remote script (notification contains port number and ID number).
Copies itself to folders that have the phrase shar in the name (such as common peer-to-peer applications; KaZaa, Bearshare, Limewire, etc)

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

CVE Links: GENERIC-MAP-NOMATCH

Reference:http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=12241
5

- **14430 W32/Bagle.aa Worm (Registry Check)**

This is a mass-mailing worm with the following characteristics:

Contains its own SMTP engine to construct outgoing messages.
Harvests email addresses from the victim machine
The From: address of messages is spoofed
Contains a remote access component (The worm sends notification via HTTP to a remote script (notification contains port number and ID number).
Copies itself to folders that have the phrase shar in the name (such as common peer-to-peer applications; KaZaa, Bearshare, Limewire, etc)

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

CVE Link: GENERIC-MAP-NOMATCH

Reference:HTTP://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=1248
75

- **14431 W32/Netsky.ab Worm (Registry Check)**

This worm:
Constructs messages using its own SMTP engine
Harvests email addresses from the victim machine
Spoofs the From: address of messages

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

CVE Link: GENERIC-MAP-NOMATCH

Reference:http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=12487
3

- **14432 W32/Netsky.aa Worm (Registry Check)**

This worm:
Constructs messages using its own SMTP engine
Harvests email addresses from the victim machine
Spoofs the From: address of messages

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

CVE Link: No CVE Match

Reference:http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=122476

- **14433 W32/Netsky.u Worm (Registry Check)**

This worm:
Constructs messages using its own SMTP engine
Harvests email addresses from the victim machine
Spoofs the From: address of messages
Opens a port on the victim machine (TCP 6789)
Delivers a DoS attack on certain web sites upon a specific date condition

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

CVE Link: No CVE Match

Reference:http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=101167

- **14434 W32/Netsky.x Worm (Registry Check)**

This worm:
Constructs messages using its own SMTP engine
Harvests email addresses from the victim machine
Spoofs the From: address of messages
Delivers a DoS attack on certain web sites upon a specific date condition

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

CVE Link: No CVE Match

Reference: http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=104475

- **17706 Fusion News Input Validation in fullnews.php Vulnerability**

It is reported that 'fullnews.php' does not filter HTML code from user-supplied input in the 'id' variable. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Fusion News software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies

(including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **Meium**

CVE Link: No CVE Match

Reference: http://securitytracker.com/alerts/2004/Apr/1009920.html

- **17707 PostNuke Downloads XSS Vulnerability**

Some vulnerabilities were reported in PostNuke. A remote user can determine the installation path. A remote user can also conduct cross-site scripting attacks.
A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the PostNuke software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.

The Downloads and Web_Links modules and the 'openwindow.php' script are reported to be vulnerable.

Test Case Impact: **Attack** Vulnerability Impact: **Attack** Risk: **Meium**

CVE Link: No CVE Match

Reference: http://www.postnuke.com/
http://securitytracker.com/alerts/2004/Apr/1009902.html

- **17887 Serv-U FTP server in the processing of the LIST -l: parameter Vulnerability**

A vulnerability in the product allows a remote user to cause the server to fail by sending a malformed LIST command to the server.

A user issuing a long parameter (around 134 bytes) as a value for a LIST command (using the -l: parameter for that LIST command), can cause the server to try and read a value that is outside the memory location of the Serv-U's memory, this will cause an exception to be triggered (an unhandled exception), which in turn causes the program to crash.

Test Case Impact: **DoS** Vulnerability Impact: **DoS** Risk: **Meium**

CVE Link: No CVE Match

Reference: http://securitytracker.com/alerts/2004/Apr/1009869.html
http://www.serv-u.com/

New Vulnerabilities found this Week

Mandrakelinux Security Update Advisory - Proftpd
MDKSA-2004:041

A portability workaround that was applied in version 1.2.9 of the ProFTPD FTP server caused CIDR based ACL entries in "Allow" and "Deny" directives to act like an "AllowAll" directive. This granted FTP clients access to files and directories that the server configuration may have been explicitly denying.

This problem only exists in version 1.2.9 and has been fixed upstream.

For more information, see:
http://www.securityfocus.com/advisories/6651
http://bugs.proftpd.org/show_bug.cgi?id=2267

Trustix Secure Linux Security Advisory - rsync
#2004-0024

Rsync uses a quick and reliable algorithm to very quickly bring remote and host files into sync. Rsync is fast because it just sends the differences in the files over the network (instead of sending the complete files). Rsync is often used as a very powerful mirroring process or just as a more capable replacement for the rcp command.

From the rsync homepage:
There is a security fix included in 2.6.1 that affects only people running a read/write daemon WITHOUT using chroot. If the user privs that such an rsync daemon is using is anything above "nobody", you are at risk of someone crafting an attack that could write a file outside of the module's "path". Please either enable chroot or upgrade to 2.6.1. People not running a daemon, running a read-only daemon, or running a chrooted daemon are totally unaffected.

For more information, see:
http://www.trustix.org/errata/misc/2004/TSL-2004-0024-rsync.asc.txt
http://www.securityfocus.com/advisories/6646

Red Hat Security Advisory - mod_ssl security issue
RHSA-2004:182-01

The Apache HTTP server is a powerful, full-featured, efficient, and freely-available Web server.

A memory leak in mod_ssl in the Apache HTTP Server prior to version 2.0.49 allows a remote denial of service attack against an SSL-enabled server. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2004-0113 to this issue.

Users of the Apache HTTP server should upgrade to these updated packages, which contain backported patches that address these issues.

For more information, see:
http://nagoya.apache.org/bugzilla/show_bug.cgi?id=27106
http://www.securityfocus.com/advisories/6640

Symantec Multiple Firewall TCP Options Denial of Service Vulnerability
Security-Corporation ID : SC-1008

eEye Digital Security has discovered a severe denial of service vulnerability in the Symantec Client Firewall products for Windows. The vulnerability allows a remote attacker to reliably render a system inoperative with one single packet. Physical access is required in order to bring an affected system out of this "frozen" state. This specific flaw exists within the component that performs low level processing of TCP packets.

For more information, see:
http://www.security-corporation.com/articles-20040424-000.html

Mandrakelinux Security Update Advisory - sysklogd
MDKSA-2004:038

Steve Grubb discovered a bug in sysklogd where it allocates an insufficient amount of memory which causes sysklogd to write to unallocated memory. This could allow for a malicious user to crash sysklogd.

For more information, see:
http://www.securityfocus.com/advisories/6636

Gentoo Linux Security Advisory - Multiple Vulnerabilities in Samba
GLSA 200404-21

Two vulnerabilities have been discovered in Samba. The first vulnerability allows a local user who has access to the smbmount command to gain root. An attacker could place a setuid-root binary on a Samba share/server he or she controls, and then use the smbmount command to mount the share on the target UNIX box. The remote Samba server must support UNIX extensions for this to work. This has been fixed in version 3.0.2a.

The second vulnerability is in the smbprint script. By creating a symlink from /tmp/smbprint.log, an attacker could cause the smbprint script to write to an arbitrary file on the system. This has been fixed in version 3.0.2a-r2.

Local users with access to the smbmount command may gain root access. Also, arbitrary files may be overwritten using the smbprint script.

For more information, see:
http://www.securityfocus.com/archive/1/353222/2004-04-09/2004-04-15/1
http://www.securityfocus.com/advisories/6635

SquirrelMail Change_Passwd Plug-in Buffer Overrun Vulnerability

The SquirrelMail change_passwd plug-in is prone to a stack-based buffer overrun vulnerability. The issue exists in the backend chpasswd binary. This vulnerability could potentially be exploited by a local user to execute arbitrary code as root.

It should be noted that the local user may need to have additional privileges to exploit this

issue, such as being a member of a special group on the system, such as webmasters or www or to have access to a special user, depending on how the software is configured.

This issue may also be remotely exploitable via the CGI interface of the software.

For more information, see:
http://www.securityfocus.com/bid/10166/discussion/

OpenSSL Denial of Service Vulnerabilities

Three security vulnerabilities have been reported to affect OpenSSL. Each of these remotely exploitable issues may result in a denial of service in applications which use OpenSSL.

The first vulnerability is a NULL pointer assignment that can be triggered by attackers during SSL/TLS handshake exchanges. The CVE candidate name for this vulnerability is CAN-2004-0079. Versions 0.9.6c to 0.9.6k (inclusive) and from 0.9.7a to 0.9.7c (inclusive) are vulnerable.

The second vulnerability is also exploited during the SSL/TLS handshake, though only when Kerberos ciphersuites are in use. The vendor has reported that this vulnerability may not be a threat to many as it is only present when Kerberos ciphersuites are in use, an uncommon configuration. The CVE candidate name for this vulnerability is CAN-2004-0112. Versions 0.9.7a, 0.9.7b, and 0.9.7c are affected.

This entry will be retired when individual BID records are created for each issue.

For more information, see:
http://www.securityfocus.com/bid/9899/discussion/

ProFTPD _xlate_ascii_write() Buffer Overrun Vulnerability

A remotely exploitable buffer overrun was reported in ProFTPD. This issue is due to insufficient bounds checking of user-supplied data in the _xlate_ascii_write() function, permitting an attacker to overwrite two bytes memory adjacent to the affected buffer. This may potentially be exploited to execute arbitrary code in the context of the server. This issue may be triggered when submitting a RETR command to the server.

For more information, see:
http://www.securityfocus.com/bid/9782/discussion/

Sun Solaris TCP/IP Networking Stack Unspecified Denial of Service Vulnerability

It has been reported that Solaris is affected by a local denial of service vulnerability that may allow an attacker to cause a system panic leading to a denial of service condition.

Due to a lack of details, further information is not available at the moment. This BID will be updated as more information becomes available.

This issue has been reported in Solaris 8 and 9.

For more information, see:
http://www.securityfocus.com/bid/10216/discussion/

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