netVigilance

ScoutNews Team **27 August 2004**
Issue #35

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Insiders are still the biggest risk to company assets.
Trojan uses phishing when compromising online bankers at most of UK's major online banks.
Polish and US officials crack down on organized online crime gangs – this is just the tip of the iceberg, however the crack down is a good and needed step in the right direction.

Enjoy reading

Top Security News Stories this Week

- **Insiders, not crooks, still biggest security threat**
  New research findings suggest that insiders - not gangs of cyber criminals - pose the biggest threat to financial service providers' systems and data.
  The Insider Threat Study, a joint initiative between the US Secret Service and Carnegie Mellon University Software Engineering Institute's CERT Coordination Center, is the first in a series of seven reports examining insider attacks on information and systems across a range of business areas.

http://www.vnunet.com/news/1157662
James Sherwood

- **Trojan targets users of British online banks, Sophos warns of latest phishing attack**
  Experts at Sophos have warned British computer users who bank online about a series of Trojan horses that try and steal financial information.
  The Tofger Trojan horses target users of a number of online banks, including Abbey, Barclays, Cahoot, HSBC, Lloyds, NatWest, Nationwide, and Woolwich.

http://www.sophos.com/virusinfo/articles/tofger.html
Sophos

- **Polish Cops Bust 100-Member Computer Piracy Gang**
  WARSAW (Reuters) - Polish police have broken up a gang of more than 100 hackers who sold pirated music and films, using academic computer systems around the world to store their wares, a police spokeswoman said on Tuesday.
  "They broke into the biggest systems they could find and set up 'warehouses' to store pirated games, films and music," police spokeswoman Agata Salatka said of one of

Poland's biggest piracy-related busts.
http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=581&e=14&u=/nm/20040824/tc_nm/crime_poland_hackers_dc
Reuters

- **Dozens of Internet Crime Suspects Nabbed**
  A summer-long effort targeting Internet crime has resulted in dozens of arrests and convictions on charges including use of "spam" e-mail to steal credit card numbers, computer hacking and online fraud, Justice Department (news - web sites) officials said Thursday.
  The suspects were identified during more than 160 federal investigations into a variety of Internet crimes that victimized about 150,000 people and caused $215 million in estimated losses, Attorney General John Ashcroft (news - web sites) said. The initiative began June 1 and ended Thursday.

http://story.news.yahoo.com/news?tmpl=story&cid=528&ncid=528&e=14&u=/ap/20040826/ap_on_hi_te/computer_crime
Curt Anderson

New Vulnerabilities Tested in SecureScout

- **13171 SARAd Buffer Overflow Vulnerability**
  SARAd program is used to serve the British National Corpus (http://www.natcorp.ox.ac.uk/SARA/).
  A vulnerability allows execution of arbitrary code over the network with the rights of the daemon.
  No authentication is required to perform an attack.
  The British National Corpus is used by many linguists for research on the English language and is licensed commercially by the BNC Consortium.
  The server software run on various flavors of Unix and is freely available in source form from http://www.natcorp.ox.ac.uk/SARA/.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.securityfocus.com/archive/1/372331/2004-08-17/2004-08-23/0 & http://www.natcorp.ox.ac.uk/SARA/index.htm

- **13170 MySQL Buffer Overflow in mysql_real_connect() Vulnerability**
  A vulnerability was reported in MySQL in mysql_real_connect(). A remote user with control over DNS may be able to cause arbitrary code to be executed on the target system.
  The software does not validate the length of user-supplied input (supplied by a DNS server) to determine if the host address will fit within the 'sock_addr.sin_addr' buffer when a reverse DNS lookup is performed. A remote user with control over the DNS or the ability to spoof the DNS may be able to supply a specially crafted return value to trigger the buffer overflow and execute arbitrary code on the target system.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://bugs.mysql.com/bug.php?id=4017

- **14463 Exchange Server 5.5 SP4 Outlook Web Access Cross-Site Scripting Vulnerability**

  Microsoft Exchange enables users to access their inboxes and other various resources located in the Web Storage System. Outlook Web Access (OWA) enables users to remotely access these resources via a URL. OWA provides Microsoft Exchange by default.
  Vulnerability has been identified, allowing malicious people to conduct script insertion attacks.
  The vulnerability is caused due to an input validation error in a HTML redirection query. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected website when a malicious entry is viewed.
  This vulnerability affects Microsoft Exchange 5.5 with Service Pack 4.

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

CVE Links: CAN-2004-0203

Reference: http://www.microsoft.com/technet/security/bulletin/ms04-026.mspx

- **15012 NetBSD ftpd Multiple Vulnerabilities**

  A set of flaws in the ftpd source code can be used together to achieve root access within an ftp session. With root file manipulation ability, mechanisms to gain a shell are numerous, so this issue should be considered a remote root situation.
  ftpd is disabled by default in NetBSD since NetBSD-1.5.3, however many users might have reason to provide this popular service.

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

CVE Link: CAN-2004-0794

Reference: http://securitytracker.com/alerts/2004/Aug/1010968.html

- **15064 Rsync sanitize path funtion module information discloasure**

  There is a path-sanitizing bug that affects daemon mode in all recent rsync versions (including 2.6.2) but only if chroot is disabled. It does NOT affect the normal send/receive filenames that specify what files should be transferred (this is because these names happen to get sanitized twice, and thus the second call removes any lingering leading slash(es) that the first call left behind). It does affect certain option paths that cause auxilliary files to be read or written.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://samba.anu.edu.au/rsync/#security_aug04 &
http://www.securityfocus.com/bid/10938

- **15067 Rsync Configured Path Directory Traversal**
  There is a security problem in all versions prior to 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" setting (where all its files should be stored). 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.

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

CVE Link: CAN-2004-0426

Reference: http://samba.anu.edu.au/rsync/#security_apr04 & http://www.securityfocus.com/bid/10247

- **15077 Rsync Daemon Mode Undisclosed Heap Overflow**
  rsync is a utility, which provides fast incremental file transfers between hosts. rsync version 2.5.6 and earlier contains a heap overflow vulnerability that can be used to remotely run arbitrary code.

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

CVE Link: CAN-2003-0962

Reference: http://samba.anu.edu.au/rsync/#security_dec03 & http://www.securityfocus.com/bid/9153

- **15018 Outdated PHP Version**
  A software component named PHP, used to dynamically generate Web pages, is outdated. Many vulnerabilities have been reported on these versions.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.php.net

- **17917 YaPiG Input Validation Code Injection Vulnerability**
  An input validation vulnerability was reported in YaPiG. A remote user can execute arbitrary operating system commands on the target system.
  It has been reported that 'add_comments.php' and 'functions.php' do not properly validate user-supplied input. A remote user can send specially crafted inputs to create a file with an arbitrary file extension and containing arbitrary contents.

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

CVE Link: GENERIC-MAP-NOMATCH

- **17918 WebAPP directory traversal Vulnerability**
  WebAPP is advertised as the internet's most feature rich, easy to run PERL based portal

system.
Several user mods are also available which ranges from chat to e-commerce applications.
Several vulnerabilities in these mods have already been discovered.
The WebAPP system itself has a serious directory traversal vulnerability.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://seclists.org/lists/bugtraq/2004/Aug/0325.html & http://www.web-app.org/

New Vulnerabilities found this Week

❖ **Gaucho "Content-Type:" Header Processing Buffer Overflow Vulnerability**
"Stack-based buffer overflow; Execution of arbitrary code"

Tan Chew Keong has reported a vulnerability in Gaucho, which can be exploited by malicious people to compromise a user's system.
The vulnerability is caused due to a boundary error within the processing of the "Content-Type:" header. This can be exploited to cause a stack-based buffer overflow via a specially crafted email containing an overly long string (about 280 characters) in the "Content-Type:" header.
Successful exploitation may allow execution of arbitrary code.
The vulnerability has been reported in version 1.4 Build 145. Other versions may also be affected.
References: http://www.security.org.sg/vuln/gaucho140.html

❖ **Cisco Secure Access Control Server Multiple Vulnerabilities**
"Denial of Service; bypass user authentication"

Multiple vulnerabilities have been reported in Cisco Secure Access Control Server (ACS), which can be exploited by malicious people to cause a DoS (Denial of Service) or bypass user authentication.
1) A connection handling error within the web-based management interface (CSAdmin) causes the interface to stop responding to requests when it is flooded with TCP connections. This may also cause other services processing authentication related requests to become unstable or stop responding.
This vulnerability affects version 3.2(2) build 15.
2) An error within the processing of LEAP (Light Extensible Authentication Procotol) authentication requests can be exploited to crash a vulnerable device.
Successful exploitation requires that the device has been configured as a LEAP RADIUS Proxy.
This vulnerability affects version 3.2.
3) An authentication error within the handling of NDS (Novell Directory Services) users can be exploited to be authenticated against a NDS database by supplying a valid username and a blank password.
Successful exploitation requires that an anonymous bind is allowed in NDS, and NDS users are authenticated with NDS as an external database.
This vulnerability affects versions 3.2(3) and prior of the ACS Solution Engine.
4) An authentication error within the ACS administration web service may allow bypassing of the authentication. The problem is that an ACS GUI is created on a random port when a

user is successfully authenticated and following only the user's IP address is used to confirm the user's identity when accessing this GUI.
This can be exploited to bypass the user authentication by accessing the ACS GUI created on a random port with a spoofed IP address matching an authenticated user.
This vulnerability affects versions 3.2(3) and prior.
The vulnerabilities affect only Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine.
References: http://www.cisco.com/warp/public/707/cisco-sa-20040825-acs.shtml

❖ **Ipswitch WhatsUp Gold's Web Server Buffer Overflow Vulnerability**
"Execution of arbitrary code"

A vulnerability has been reported in Ipswitch WhatsUp Gold's web server, which can be exploited by malicious people to compromise a vulnerable system.
The problem is caused due to a boundary error in the script "_maincfgret.cgi". This can be exploited by sending a specially crafted HTTP POST request containing an overly long value for the "instancename" parameter.
Successful exploitation may allow execution of arbitrary code.
The vulnerability has been reported in version 8.03. Other versions may also be affected.
NOTE: The Ipswitch WhatsUp Gold's web server is not enabled by default.
References: http://www.idefense.com/applicat...?id=133&type=vulnerabilities

❖ **Winamp Skin File Arbitrary Code Execution Vulnerability**
"Execute arbitrary programs"

A vulnerability has been reported in Winamp, which can be exploited by malicious people to compromise a user's system.
The problem is caused due to insufficient restrictions on Winamp skin zip files (.wsz). This can e.g. be exploited by a malicious website using a specially crafted Winamp skin to place and execute arbitrary programs. With Internet Explorer this can be done without user interaction.
An XML document in the Winamp skin zip file can reference a HTML document using the "browser" tag and get it to run in the "Local computer zone". This can be exploited to run an executable program embedded in the Winamp skin file using the "object" tag and the "codebase" attribute.
NOTE: The vulnerability is reportedly being exploited in the wild.
The vulnerability has been confirmed on a fully patched system with Winamp 5.04 using Internet Explorer 6.0 on Microsoft Windows XP SP1.
References: http://www.k-otik.net/bugtraq/08262004.Winamp.php

❖ **NSS Library SSLv2 Connection Negotiation Buffer Overflow Vulnerability**
"Heap-based buffer overflow; Execution of arbitrary code"

ISS X-Force has reported a vulnerability in the NSS library, which can be exploited by malicious people to compromise a vulnerable system.
The vulnerability is caused due to a boundary error within the parsing of records during SSLv2 connection negotiation. This can be exploited to cause a heap-based buffer overflow by sending a specially crafted client hello message with an overly long record.
Successful exploitation allows execution of arbitrary code with the privileges of an application linked to the vulnerable library.
References: http://xforce.iss.net/xforce/alerts/id/180

❖ **Painkiller Password Processing Buffer Overflow Vulnerability**

"Buffer overflow; Execution of arbitrary code"

Luigi Auriemma has reported a vulnerability in Painkiller, which potentially can be exploited by malicious people to compromise a vulnerable system.
The vulnerability is caused due to a boundary error in the server when processing a password supplied by a client during the connection establishment. This can be exploited to cause a buffer overflow by sending a packet with an overly long string in the password field to a vulnerable server.
Successful exploitation may potentially allow execution of arbitrary code.
The vulnerability has been reported in version 1.3.1 and prior.
References: http://aluigi.altervista.org/adv/painkex-adv.txt

❖ **WebAPP Directory Traversal Vulnerability**

"Retrieve arbitrary files outside the web root via directory traversal attacks"

A vulnerability has been reported in WebAPP, which can be exploited by malicious people to access sensitive information.
The problem is caused due to an input validation error in "cgi-bin/cgi-lib/topics.pl", making it possible to retrieve arbitrary files outside the web root via directory traversal attacks.
The vulnerability has been reported in version 0.9.9.1. Other versions may also be affected.
References: http://seclists.org/lists/bugtraq/2004/Aug/0325.html

❖ **xv Multiple Buffer Overflow Vulnerabilities**

"Buffer overflows; Execution of arbitrary code"

infamous41md has reported multiple vulnerabilities in xv, which potentially can be exploited by malicious people to compromise a user's system.
The vulnerabilities are caused due to boundary errors within the processing of images and can be exploited to cause buffer overflows by tricking users into viewing specially crafted images.
Successful exploitation may allow execution of arbitrary code on a user's system.
The vulnerabilities have been reported in version 3.10a. Other versions may also be affected.
References: http://www.1nfamus.netfirms.com/xv_advisory.html

❖ **BNC SARA Buffer Overflow Vulnerabilities**

"Boundary errors"

Matthias Bethke has reported some vulnerabilities in SARA from British National Corpus, which can be exploited by malicious people to compromise a vulnerable system.
The vulnerabilities are caused due to boundary errors in the sarad daemon when parsing traffic from clients. This can be exploited by sending a specially crafted, overly long string to the sarad daemon.
References: http://secunia.com/advisories/12348/

❖ **Microsoft Internet Explorer MHTML Content-Location Cross Security Domain Scripting Vulnerability**

"Executing script in the intra-net security Zone"

Microsoft Internet Explorer is reported prone to a cross security domain scripting vulnerability. The issue is reported to present itself when a malicious MHTML file is rendered.
A proof of concept for this issue employs Content-Location attributes in a MHTML file that are sufficient to trick Internet Explorer into executing script contained in the MHTML file in the intra-net security Zone.
This issue is reported to affect Microsoft Internet Explorer when it is installed on a computer that is running Microsoft Windows XP Service Pack 2.
References: http://www.securityfocus.com/bid/10979/

❖ **EGroupWare Multiple Input Validation Vulnerabilities**
"Cross-site scripting; Theft of cookie-based authentication credentials"

It is reported that eGroupWare is susceptible to multiple cross-site scripting and HTML injection vulnerabilities.
The cross-site scripting issues present themselves in the various parameters of the 'addressbook' and 'calendar' modules. It is also reported that data input through the 'Search' fields of the 'addressbook', 'calendar', and 'search between projects' functionality are not sufficiently sanitized.
An attacker can exploit these issues for theft of cookie-based authentication credentials and other attacks.
Additionally HTML injection vulnerabilities are reported for the eGroupWare 'Messenger' module and 'Ticket' module.
Attackers may potentially exploit these issues to manipulate web content or to steal cookie-based authentication credentials. It may be possible to take arbitrary actions as the victim user.
References: http://www.securityfocus.com/bid/11013/

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