netVigilance

ScoutNews Team **16 August 2004**
Issue #33

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

As Yahoo needs to patch a new release of its IM software we see newer players in the market betting on the proliferation of secure IM in government and corporate accounts.

An upsurge is seen in SPAM and it is speculated that it is a mechanism of supply and demand.

McAfee is warning that hackers are keeping up and society's are ever more vulnerable as McAfee buys Foundstone to help their customers.

Microsoft's firewall that is on by default for all users that apply service pack 2 for Windows XP is applauded for being on by default, but criticized for not having all the right features.

Enjoy reading

Top Security News Stories this Week

- **Yahoo! IM security hole gets patch after website warning**

Graphical malware stopped in its tracks

Yahoo! issued a security patch to fix a potential vulnerability in its latest instant messaging software, the company has announced.
The patch repairs a security hole stemming from Yahoo! Messenger's use of the portable network graphics - or PNG - format, an open-source code the program uses to display certain images, such as buddy list avatars.
The most critical issue, a memory problem known as a buffer overflow, could allow specially created PNG graphics to execute malicious programs when a vulnerable application loads an image.
http://software.silicon.com/security/0,39024655,39123191,00.htm
Jim Hu

- **Summer of Love Prompts Salacious Spam Upsurge; While Zafi-B Tops Clearswift's Virus Index**

As the temperature rises, spam is also heating up, according to Clearswift's latest spam index. Levels of pornographic e-mails have shot up by almost 350% since June, and in what appears to be an attempt to match supply with demand, healthcare spam

(most of which was Viagra) has also risen significantly.
This upsurge is reminiscent of the same period last year -- spammers appear to be purposefully increasing their pornographic output during the summer months. IT managers are warned to be particularly vigilant to guard against damage to company reputation caused by the circulations of inappropriate images.
http://www.tmcnet.com/usubmit/2004/Aug/1065737.htm
TMC

- **Antepo and SPYRUS Partner to Deliver the Industry's Most Secure Instant Messaging System to Government and Private Sectors**

SPYRUS to Integrate Antepo's OPN System into Its Suite of End-to-End Security Solutions to Add Interoperable IM and Collaboration Capabilities
Antepo, Inc. (www.antepo.com), a pioneer of secure, interoperable Enterprise Instant Messaging (EIM), together with SPYRUS®, Inc., a leading provider of high assurance security products, today announced a partnership to provide a suite of highly reliable, interoperable instant messaging and collaboration products that meet the stringent security requirements of corporate and government organizations worldwide. As part of the Antepo Partner Network™, SPYRUS will integrate Antepo's Open Presence Network™ technology into its hardware-based cryptographic systems used to secure and manage a wide variety of activities requiring authentication and controlled access to data on enterprise networks.
http://www.tmcnet.com/usubmit/2004/Aug/1065690.htm
TMC

- **Security expert warns computer hackers keeping up with technology**

Computer hackers are keeping up with the times and are putting an increasingly technology-dependent world at risk, the chairman of leading US-based IT security firm McAfee said.
"The telecom infrastructure -- whether it be routing in India, UK, Germany or US -- is at risk, " George Samenuk told a business conference in Bombay.
"When cellphones go down, it is 10 times as worse because the whole world revolves around cellphones nowadays," he said.
http://story.news.yahoo.com/news?tmpl=story&ncid=1209&e=5&u=/afp/20040816/tc_afp/india_us_technology&sid=96001015
AFP

- **Microsoft firewall could be security risk**

IT security experts and vendors this week welcomed the introduction of Windows Firewall, part of Windows XP Service Pack 2 (SP2), as a valuable way of protecting PCs. But while the firewall is an improvement, it falls short of the standard of protection expected of commercial firewalls, according to some industry observers.
Windows Firewall -- which replaces the old Internet Connection Firewall -- marks the first time all up-to-date PCs will have a firewall switched on by default, an important step in stopping the spread of viruses, according to industry analysts. However, the software suffers from two major flaws, critics say: it does not block outbound traffic, and it can be switched off by another application, possibly even by a clever worm.
http://security.itworld.com/4362/040816msfirewall/page_1.html
Mathew Broersma

New Vulnerabilities Tested in SecureScout

- **14462 Cumulative Security Update for Internet Explorer (MS04-025/867801)**

  Navigation Method Cross-Domain Vulnerability - CAN-2004-0549:
  A remote code execution vulnerability exists in Internet Explorer because of the way that it handles navigation methods. An attacker could exploit the vulnerability by constructing a malicious web page that could potentially allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could run malicious script code in the Local Machine security zone in Internet Explorer. If a user is logged on with administrative privileges, this could allow the attacker to take complete control of an affected system.

  Malformed BMP File Buffer Overrun Vulnerability - CAN-2004-0566:
  A buffer overrun vulnerability exists in the processing of BMP image file formats that could allow remote code execution on an affected system. If the user is logged on with administrative privileges an attacker who successfully exploited this vulnerability could take complete control of the affected system. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

  Malformed GIF File Double Free Vulnerability - CAN-2003-1048:
  Abuffer overrun vulnerability exists in the processing of GIF image file formats that could allow remote code execution on an affected system. If the user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the affected system. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

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

CVE Links: CAN-2004-0549 & CAN-2004-0566 & CAN-2003-1048

Reference: http://www.microsoft.com/technet/security/bulletin/MS04-025.mspx

- **17913 thttpd Directory Traversal Vulnerability**
  Vulnerability exists in the Windows port of thttpd. A remote user can view files on the target system that are located outside of the web document directory.

  The software does not properly validate user-supplied requests. A remote user can submit a request containing directory traversal characters or a direct path to view files on the system.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.securitytracker.com/alerts/2004/Aug/1010850.html & http://www.acme.com/software/thttpd/thttpd.html

- **17914 IBM Directory Server 'ldacgi' Directory Traversal Vulnerability**
  Vulnerability exists in the IBM Directory Server in 'ldacgi.exe'. A remote user can view files on the target system with the privileges of the web service.

  'ldacgi.exe' script does not properly validate user-supplied input in the 'Template' parameter. A remote user can supply a path containing directory traversal characters ('../') to view arbitrary files on the target system.

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

CVE Links: GENERIC-MAP-NOMATCH

Reference: http://www.securitytracker.com/alerts/2004/Aug/1010834.html & http://www.ibm.com/support/docview.wss?uid=isg1IR52692

- **17915 eNdonesia 'mod.php' XSS Vulnerability**
  eNdonesia does not properly filter HTML code from user-supplied input in the "query" parameter. 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 eNdonesia portal 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: **Medium**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.securitytracker.com/alerts/2004/Aug/1010864.html & http://sourceforge.net/projects/endonesia

- **17916 Moodle 'post.php' Cross Site Scripting Vulnerability**
  An input validation vulnerability exists in Moodle in 'post.php'. A remote user can conduct cross-site scripting attacks.

  Script 'post.php' does not properly filter HTML code from user-supplied input in the reply 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 Moodle 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: **Medium**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.securitytracker.com/alerts/2004/Aug/1010893.html

- **19066 Adware Bonzi**
  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: L**ow**

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/b/bonzi.asp

- **19067 Adware BookmarkExpress**
  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/b/bookmarkexpress.asp

- **19068 Adware BrowserToolbar**
  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/b/browsertoolbar.asp

- **19069 Adware BuddyLinks**
  Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not displayed within the form of an ad-sponsored application. Some Adware may hijack the ads of other companies, replacing them with its own.

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

CVE Link: GENERIC-MAP-NOMATCH

Reference: http://www.pestpatrol.com/pestinfo/b/buddylinks.asp

New Vulnerabilities found this Week

- **Adobe Acrobat Reader ActiveX Control Buffer Overflow Vulnerability**

"Execute arbitrary code"

Rafel Ivgi has reported a vulnerability in Adobe Acrobat Reader, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the "pdf.ocx" ActiveX component supplied with Adobe Acrobat Reader. This can e.g. be exploited via a malicious website using a specially crafted URL to potentially execute arbitrary code.

The vulnerability has been reported in version 5.0.5. Other versions may also be affected.

References:
http://www.idefense.com/application/poi/display?id=126&type=vulnerabilities&flashstatus=true

- **Internet Explorer Address Bar Spoofing Vulnerability**

"Phishing attacks against a user"

Liu Die Yu has discovered a vulnerability in Internet Explorer, which potentially can be exploited by malicious people to conduct phishing attacks against a user.

The vulnerability is caused due to Internet Explorer failing to update the address bar after a sequence of actions has been performed on a named window. This can be exploited to display content from a malicious site while displaying the URL of a trusted site in the address bar.

The vulnerability has been confirmed on a fully patched system with Internet Explorer 6 running on Microsoft Windows 2000 SP4 / Microsoft Windows XP SP1.

Previous versions of Internet Explorer may also be affected.
Currently known attack vectors do not work on Windows XP systems with SP2 applied.

References:
http://secunia.com/advisories/12304/

- **Adobe Acrobat Reader Shell Command Injection and Buffer Overflow Vulnerability**

"Injection of arbitrary shell commands, buffer overflow"

Greg MacManus has reported two vulnerabilities in Adobe Acrobat Reader, which can be exploited by malicious people to compromise a user's system.

1) An input validation error within the "uudecoding" feature allows injection of arbitrary shell commands. This can be exploited via a malicious PDF document with a specially crafted filename containing backtick shell metacharacters.

2) A boundary error within the "uudecoding" feature can be exploited to cause a buffer overflow via a malicious PDF document with an overly long filename.

Successful exploitation may allow execution of arbitrary code, but requires that a user is tricked into opening a malicious document.

The vulnerabilities have been reported in versions 5.05 and 5.06 for UNIX. Other versions may also be affected.

References:
http://www.idefense.com/applicat...?id=124&type=vulnerabilities
http://www.idefense.com/applicat...?id=125&type=vulnerabilities

- **Gaim Unspecified MSN Protocol Buffer Overflow Vulnerabilities**

"Buffer overflows"

Sebastian Krahmer has discovered some vulnerabilities in gaim, which can potentially be exploited by malicious people to compromise a user's system.

The vulnerabilities are caused due to boundary errors within the parsing functions for the MSN protocol and can be exploited to cause buffer overflows.

Successful exploitation may allow execution of arbitrary code.

References:
http://securitytracker.com/alerts/2004/Aug/1010872.html

- **SpamAssassin Message Handling Denial of Service Vulnerability**

"Denial of Service"

A vulnerability has been discovered in SpamAssassin, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an unspecified error within the processing of certain malformed messages.

References:
http://secunia.com/advisories/12255/

- **AOL Instant Messenger "Away" Message Buffer Overflow Vulnerability**

"Stack-based buffer overflow"

Ryan McGeehan has reported a vulnerability in AOL Instant Messenger (AIM), which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error within the handling of "Away" messages and can be exploited to cause a by supplying an overly long "Away" message (about 1024 bytes). A malicious website can exploit this via the "aim:" URI handler by passing an overly long argument to the "goaway?message" parameter.

Successful exploitation allows execution of arbitrary code on a user's system when e.g. a malicious website is visited with certain browsers.

The vulnerability has been confirmed in version 5.5.3595. Other versions may also be affected.

NOTE: Various other issues were also reported, where a large amount of resources can be consumed on a user's system.

References:
http://www.idefense.com/applicat...?id=121&type=vulnerabilities
http://www.kb.cert.org/vuls/id/735966

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