netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 40

October 6, 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.

This Week in Review

Security providers fear Vista. Economic crime based on hacking on the rise. VoIP and security. A little cry of despair.

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

- **Microsoft's New Security Problem: McAfee**

It appears that McAfee doesn't really want anyone solving computer security problems other than itself. That's a normal frame of mind for any ambitious company, but that attitude becomes dangerous when governments buy into it and start to deploy the power of the state to implement it.
For years, Microsoft (Nasdaq: MSFT) Latest News about Microsoft has come under heavy fire for not making its systems secure enough. Now, with the upcoming release of its new operating system (OS), Windows Vista, the company is being unfairly attacked by self-

interested competitors for adding more security to protect consumers.

Back in 2002, when Microsoft co-founder Bill Gates announced that the company would be making security a priority, the computing industry responded with a collective, "Finally." Thomas Greene, writing for the Register, reported at the time that "Bill finally admits that the company has wrongly emphasized whistles and bells over security, and decrees that this shall change." He went on to say, "Hallelujah. He's finally arrived on the same page as the rest of the computing world."
Going to Extremes

Greene's analysis Track Customer Satisfaction with Online Surveys would have been more accurate if he had written, "the rest of the computing world except for those who will lose business when consumers' computing lives become more secure."

TechNewsWorld

Full Story :
http://www.technewsworld.com/story/BBLGrl2bv7xEF1/Microsofts-New-Security-Problem-McAfee.xhtml

❖ Russian online blackmailers jailed

Authorities in Russia have jailed a gang who blackmailed online companies through distributed denial-of-service (DDoS) attacks. Russian authorities worked with the UK National High Tech Crime Unit, Interpol, and the FBI to apprehend the gang.

The gang is said to have extorted more than two million pounds sterling from British online casinos and betting shops after threatening to attack their websites, making them inaccessible to the outside world. Victims of the online blackmail gang included Canbet Sports Bookmakers, who refused to pay a 5,000 pound ransom demand and found their website had been taken out of action by the hackers during the Breeders' Cup Races, losing them more than 100,000 pounds in lost business for each day of downtime.

According to prosecutors, the gang made over 50 similar blackmail attacks in 30 different countries during their six months of activity.

Ivan Maksakov, Alexander Petrov, and Denis Stepanov were each sentenced to eight years in prison and a fine of nearly 2,000 pounds.

"Malicious DDoS attacks on commercial websites can cause serious financial damage to the businesses affected, and are a major nuisance to internet users," said Graham Cluley, senior technology consultant at Sophos. "These sentences should send a strong message to other internet hackers considering online blackmail, that they can expect stiff sentences if caught. However, many gangs may believe that the relative anonymity of the internet gives them carte blanche to carry on. All computer users should ensure that they have secure defences in place to protect against abuse like this."

SecurityPark.net

Full Story :
http://www.securitypark.co.uk/article.asp?articleid=25923&CategoryID=1

- **The myths and realities of VoIP security**

Security is often cited as one of the primary reasons organisations have not deployed VoIP. Network managers need to cut through the hype and deploy the right security to maximise the reliability of the voice network and have a successful rollout.

The shift to VoIP changes many things. With voice the old TDM way, the PBX was a stand alone closed system with phones directly connected into them. Its simplicity was also its security. Of course, the problem with this model is that sharing applications was difficult; moves, adds and changes were expensive and there was no integration with the data network. A VoIP system looks a lot like any other networked application. There's a call server, mail server and other applications running on commercially available hardware with IP endpoints that communicate with it. These servers and end points communicate via an IP-over -Ethernet network connected with switches and routers.

Since a VoIP system parallels other IP applications, the threats to it are similar and require an understanding of how the VoIP components are impacted.

Computerweekly.com

Full Story :
http://www.computerweekly.com/Articles/2006/10/02/218965/The+myths+and+realities+of+VoIP+security.htm

- **The sad state of computer security**

The reality of IT security is dismal -- and there's little hope in sight for improvement

I teach computer security for a living. Last week, a class of mine asked which vendor had the best security. I responded that they all are pretty bad. If you aren't using OpenBSD or software by D.J. Bernstein, then every other product in the world is pretty bad in comparison.

Most software contains numerous vulnerabilities, holes, and exploitable routines. Even our anti-malware software and devices, the things that are supposed to protect us, are full of buffer overflows and vulnerabilities. All Internet browsers are full of holes.

The world of computer security is so much worse than the average Internet user or politician believes. Bots own tens of millions of computers at any single point in time. The people who make a living at closing tens to hundreds of thousands of bot-infected computers a day readily admit that they are not making a dent in the bad guy's ability to use bots for crime.

InfoWorld

Full Story :
http://www.infoworld.com/article/06/10/06/41OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/06/10/06/41OPsecadvise_1.html

New Vulnerabilities Tested in SecureScout

- **12142 OpenSSH Signal Handling Vulnerability**

Mark Dowd reported a vulnerability in OpenSSH, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise of a vulnerable system.

The vulnerability is caused due to a race condition within the signal handling. This can be exploited to crash the OpenSSH server and potentially allows the execution of arbitrary code.

The vulnerability has been reported in version 4.3. Prior versions may also be affected.

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

References:

Original advisory:
http://openssh.org/txt/release-4.4

Other references:
MLIST:[openssh-unix-dev] 20060927 Announce: OpenSSH 4.4 released
URL:http://marc.theaimsgroup.com/?l=openssh-unix-dev&m=115939141729160&w=2
FREEBSD:FreeBSD-SA-06:22.openssh
URL:ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:22.openssh.asc
REDHAT:RHSA-2006:0698
URL:http://www.redhat.com/support/errata/RHSA-2006-0698.html
REDHAT:RHSA-2006:0697
URL:http://www.redhat.com/support/errata/RHSA-2006-0697.html
SLACKWARE:SSA:2006-272-02
URL:http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.592566
UBUNTU:USN-355-1
URL:http://www.ubuntu.com/usn/usn-355-1
BID:20241
URL:http://www.securityfocus.com/bid/20241
SECTRACK:1016940
URL:http://securitytracker.com/id?1016940
SECUNIA:22158
URL:http://secunia.com/advisories/22158
SECUNIA:22173
URL:http://secunia.com/advisories/22173
SECUNIA:22183
URL:http://secunia.com/advisories/22183
SECUNIA:22196
URL:http://secunia.com/advisories/22196
SECUNIA:22236
URL:http://secunia.com/advisories/22236
XF:openssh-signal-handler-race-condition(29254)
URL:http://xforce.iss.net/xforce/xfdb/29254

Product homepage:
http://www.openssh.com/

CVE Reference: CVE-2006-5051

❖ 12143 OpenSSH usernames validity determination Vulnerability

Unspecified vulnerability in portable OpenSSH before 4.4, when running on some platforms, allows remote attackers to determine the validity of usernames via unknown vectors involving a GSSAPI "authentication abort."

The vulnerability has been reported in version 4.3. Prior versions may also be affected.

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

References:

Original advisory:
http://openssh.org/txt/release-4.4

Other references:
URL:http://marc.theaimsgroup.com/?l=openssh-unix-dev&m=115939141729160&w=2
REDHAT:RHSA-2006:0697
URL:http://rhn.redhat.com/errata/RHSA-2006-0697.html
SLACKWARE:SSA:2006-272-02
URL:http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.592566
BID:20245
URL:http://www.securityfocus.com/bid/20245
SECTRACK:1016939
URL:http://securitytracker.com/id?1016939
SECUNIA:22158
URL:http://secunia.com/advisories/22158
SECUNIA:22173
URL:http://secunia.com/advisories/22173

Product homepage:
http://www.openssh.com/

CVE Reference: CVE-2006-5052

❖ 13436 Skype URL Handling File Disclosure Vulnerability (Remote File Checking)

Skype is a free program that uses the latest P2P (cutting edge p2p technology) technology to bring affordable and high-quality voice communications.

A vulnerability has been reported in Skype, which can be exploited by malicious people to bypass certain security restrictions and potentially disclose certain sensitive information.

The vulnerability is cause due to an error within the parsing of the parameters passed by the URI handler. This can be exploited to inject additional command line switches to the Skype client to initiate transfer of a file from one Skype user to another via a

specially crafted Skype URL, without requiring the sender to explicitly consent the action.

Successful exploitation requires that the user follows a malicious Skype URL and that the recipient has previously authorised the sender.

The vulnerability has been reported in the following versions of Skype for Windows.
* Release 2.0.*.104 and prior
* Release 2.5.*.0 through 2.5.*.78

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

References:

Original advisories:
http://www.skype.com/security/skype-sb-2006-001.html

Other references:
CERT-VN:VU#466428
URL:http://www.kb.cert.org/vuls/id/466428
BID:18038
URL:http://www.securityfocus.com/bid/18038
FRSIRT:ADV-2006-1871
URL:http://www.frsirt.com/english/advisories/2006/1871
SECUNIA:20154
URL:http://secunia.com/advisories/20154
XF:skype-uri-handler-file-access(26557)
URL:http://xforce.iss.net/xforce/xfdb/26557

Product Home Page:
http://www.skype.com/

CVE Reference: CVE-2006-2312

❖ 16348 PHP "open_basedir" Symlink Security Bypass Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

Stefan Esser has reported a vulnerability in PHP, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to a race condition in the handling of symlinks and can be exploited to bypass the open_basedir protection mechanism.

The vulnerability has been reported in PHP4 < 4.4.4 and PHP5 < 5.1.6.

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

References:

Original Advisory:

http://www.hardened-php.net/advisory_082006.132.html

Other references:
http://www.php.net/release_4_4_4.php
http://www.php.net/release_5_1_6.php

Product Page:
http://www.php.net/

CVE Reference:

❖ 16349 PHP "_ecalloc" Integer Overflow Vulnerability

PHP is the Personal HomePage development toolkit, distributed by the PHP.net, and maintained by the PHP Development Team in public domain.

A vulnerability has been reported in PHP, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

The vulnerability is caused due to an integer overflow within the "_ecalloc" function. This can potentially be exploited to execute arbitrary code via specially crafted requests if a PHP script allocates memory based on attacker supplied data.

The vulnerability has been reported in PHP4 < 4.4.4 and PHP5 < 5.1.6.

NOTE: This vulnerability is reportedly being exploited in the wild.

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

References:

Original Advisory:
http://cvs.php.net/viewvc.cgi/ZendEngine2/zend_alloc.c?r1=1.161&r2=1.162

Other references:
N.A.

Product Page:
http://www.php.net/

CVE Reference: CVE-2006-4812

❖ 18116 MailEnable boundary error within the processing of the signature field of a NTLM Type 1 message Vulnerability

A vulnerability has been reported in MailEnable, which can be exploited by malicious people to potentially compromise a vulnerable system.

A boundary error within the processing of the signature field of a NTLM Type 1 message can be exploited to cause a buffer overflow and may allow execution of arbitrary code.

The vulnerability has been reported in MailEnable Professional 2.0 and MailEnable Enterprise 2.0.
Other versions may also be affected.

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

References:

Original advisory:
http://labs.musecurity.com/advisories/MU-200609-01.txt

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

CVE Reference:

❖ 18117 MailEnable boundary error within the processing of base64 encoded NTLM Type 1 messages Vulnerability

A vulnerability has been reported in MailEnable, which can be exploited by malicious people to potentially compromise a vulnerable system.

A boundary error within the processing of base64 encoded NTLM Type 1 messages can be exploited to cause a DoS.

The vulnerability has been reported in MailEnable Professional 2.0 and MailEnable Enterprise 2.0.
Other versions may also be affected.

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

References:

Original advisory:
http://labs.musecurity.com/advisories/MU-200609-01.txt

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

CVE Reference:

❖ 18118 MailEnable boundary error within the decoding of base64 encoded Type 3 messages Vulnerability

A vulnerability has been reported in MailEnable, which can be exploited by malicious people to potentially compromise a vulnerable system.

A boundary error within the decoding of base64 encoded Type 3 messages can

potentially be exploited to execute arbitrary code.

The vulnerability has been reported in MailEnable Professional 2.0 and MailEnable Enterprise 2.0.
Other versions may also be affected.

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

References:

Original advisory:
http://labs.musecurity.com/advisories/MU-200609-01.txt

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

CVE Reference:

❖ 18119 MailEnable SPF Lookup Denial of Service Vulnerability

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

The vulnerability is caused due to a NULL pointer dereference error in the SMTP service when under certain circumstances processing SPF lookups. This can be exploited by performing an SPF lookup for a domain with large records.

Successful exploitation crashes the SMTP service.

The vulnerability has been reported in MailEnable Professional 2.0 and MailEnable Enterprise 2.0.
Other versions may also be affected.

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

References:

Original advisory:
http://www.mailenable.com/hotfix/
http://www.mailenable.com/hotfix/MESMTPC.ZIP

Other references:
BID:20091
URL:http://www.securityfocus.com/bid/20091
FRSIRT:ADV-2006-3669
URL:http://www.frsirt.com/english/advisories/2006/3669
SECTRACK:1016792
URL:http://securitytracker.com/id?1016792
SECUNIA:21998
URL:http://secunia.com/advisories/21998
XF:mailenable-spf-dos(28910)
URL:http://xforce.iss.net/xforce/xfdb/28910

Product Homepage:

http://www.mailenable.com/

CVE Reference: CVE-2006-4616

❖ 18120 MailEnable SMTP Service HELO Denial of Service Vulnerability

DivisionByZero has reported a vulnerability in MailEnable, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the SMTP service when handling the HELO command. This can be exploited to crash the service via a HELO command with specially crafted arguments.

The vulnerability has been reported in MailEnable Professional 2.0 and MailEnable Enterprise 2.0.
Other versions may also be affected.

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

References:

Original advisory:
http://www.divisionbyzero.be/?p=173
http://www.divisionbyzero.be/?p=174

Other references:
BUGTRAQ:20060624 Mailenable SMTP Service DoS
URL:http://www.securityfocus.com/archive/1/archive/1/438374/100/0/threaded
CONFIRM: http://www.mailenable.com/hotfix/mesmtpc.zip
BID:18630
URL:http://www.securityfocus.com/bid/18630
FRSIRT:ADV-2006-2520
URL:http://www.frsirt.com/english/advisories/2006/2520
OSVDB:26791
URL:http://www.osvdb.org/26791
SECTRACK:1016376
URL:http://securitytracker.com/id?1016376
SECUNIA:20790
URL:http://secunia.com/advisories/20790
XF:mailenable-smtp-helo-dos(27387)
URL:http://xforce.iss.net/xforce/xfdb/27387

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

CVE Reference: CVE-2006-3277

New Vulnerabilities found this Week

McAfee ePolicy Orchestrator / ProtectionPilot Source Header Buffer Overflow
"Execute arbitrary code"

A vulnerability has been reported in McAfee ProtectionPilot and McAfee ePolicy Orchestrator, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error within the handling of long source headers. This can be exploited to cause a buffer overflow and potentially allows executing arbitrary code by sending a specially crafted request to a vulnerable system.

The vulnerability has been reported in McAfee ProtectionPilot 1.1.0 and McAfee ePolicy Orchestrator 3.5.0. Other versions may also be affected.

References:
http://download.nai.com/products/patches/protectionpilot/v1.1.1/PRP1113.txt
http://download.nai.com/products/patches/ePO/v3.5/EPO3506.txt

Skype URI Argument Handling Format String Vulnerability
"allow execution of arbitrary code**"**

Tom Ferris has reported a vulnerability in Skype for Mac, which potentially can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a format string error within the handling of URI arguments and can be exploited via a specially crafted Skype URL containing format specifiers.

Successful exploitation may allow execution of arbitrary code.

The vulnerability affects versions 1.5.*.79 and prior.

References:
http://www.skype.com/security/skype-sb-2006-002.html
http://www.security-protocols.com/sp-x34-advisory.php
http://descriptions.securescout.com/tc/13436

PHP "_ecalloc" Integer Overflow Vulnerability
"Denial of Service"

A vulnerability has been reported in PHP, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system.

The vulnerability is caused due to an integer overflow within the "_ecalloc" function. This can potentially be exploited to execute arbitrary code via specially crafted requests if a PHP script allocates memory based on attacker supplied data.

References:
http://cvs.php.net/viewvc.cgi/ZendEngine2/zend_alloc.c?r1=1.161&r2=1.162
http://descriptions.securescout.com/tc/16349

PHP "open_basedir" Symlink Security Bypass Vulnerability

"Bypass the open_basedir protection mechanism"

Stefan Esser has reported a vulnerability in PHP, which can be exploited by malicious, local users to bypass certain security restrictions.

The vulnerability is caused due to a race condition in the handling of symlinks and can be exploited to bypass the open_basedir protection mechanism.

The vulnerability has been reported in PHP4 and PHP5.

References:
http://www.hardened-php.net/advisory_082006.132.html
http://descriptions.securescout.com/tc/16348

GroupWise Messenger Blowfish Zero-Sized Strings Denial of Service

"Denial of Service"

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

The vulnerability is caused due to a NULL pointer dereference error within the blowfish routines when handling zero-sized strings. This can be exploited to crash the service via a specially crafted HTTP POST request with a modified "val" parameter.

The vulnerability is reported in GroupWise 1.0.6 and 2.02 Messenger Agents. Other versions may also be affected.

References:
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2974452.htm
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2974440.htm
http://idefense.com/intelligence/vulnerabilities/display.php?id=416

MailEnable Multiple Vulnerabilities

"Denial of Service"

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

1) A boundary error within the processing of the signature field of a NTLM Type 1 message can be exploited to cause a buffer overflow and may allow execution of arbitrary code.

2) A boundary error within the processing of base64 encoded NTLM Type 1 messages can be exploited to cause a DoS.

3) A boundary error within the decoding of base64 encoded Type 3 messages can potentially be exploited to execute arbitrary code.

The vulnerabilities have been reported in MailEnable Professional 2.0 and MailEnable Enterprise 2.0. Other versions may also be affected.

References:
http://labs.musecurity.com/advisories/MU-200609-01.txt

http://descriptions.securescout.com/tc/18116
http://descriptions.securescout.com/tc/18117
http://descriptions.securescout.com/tc/18118

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