ScoutNews Team **June 3, 2005**
Issue # 22

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

BofA rolls new anti-phishing technology, Texas Congressman seeks to squelch Wi-Fi freedom. New Bagle tri-fecta poses serious threat.

Enjoy reading

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **Bank of America Sitekey proposes to reduce Phishing**

SiteKey uses a combination of an image, user-created phrase and three challenge questions to authenticate both the customer's identity and the authenticity of Bank of America's Web site when customers log on to a Bank of America website.

Two-way authentication technology from PassMark Security is employed to present information containing a phrase and a picture that is only know to the account holder. As with all new security innovations; it has drawn detractions and will definitely invoke hackers to try and break it.

Related LInks :

http://www.eweek.com/article2/0,1759,1821126,00.asp

http://www.redherring.com/Article.aspx?a=12088&hed=RH-100:+Democratizing+Encryption

http://news.com.com/2061-10789_3-5723556.html?part=rss&tag=5723556&subj=news

- **Republican congressman from Texas proposes ban on free wireless access points.**

The bill, HR 2726, is similar to a host of state bills pushed by telecommunications companies aimed at fending off municipally-run wireless networks.

I am sure it is pure coincidence that the bill's author; Representative Pet Sessions (R-Texas) is a former Southwestern Bell employee, Hmmmm.
Mobile Pipeline

Full Story:
http://www.mobilepipeline.com/showArticle.jhtml?articleID=164300100

- **New threat described as spread, disarm, and exploit; bodes of more sophisticated hacker attacks.**

The attack is initiated using a Bagle variant; Glieder, which doesn't spread on its own. Glieder is spread via massive Spam attacks. Glieder then downloads a Trojan known as Fantibag, this Trojan conducts a "shields down" attack; isolating the target system from security resources such as anti-virus websites, Windows update, etc. A third Bagle variant: Mitglieder is then loaded which turns the machine into a spam proxy and also installs a backdoor for the hackers to further exploit the system.
TechWeb News

Full Story:
http://www.informationweek.com/story/showArticle.jhtml;jsessionid=5HDLGGSBL3AFEQSNDBCCKH0CJUMEKJVN?articleID=163703279&tid=6004

New Vulnerabilities Tested in SecureScout

- **15206 Symantec Brightmail AntiSpam Static Database Password Vulnerability (Remote File Checking)**

  A security issue has been reported in Symantec Brightmail AntiSpam, which can be exploited by malicious people to bypass security restrictions.

  The security issue is caused due to a static database administration password, which can be exploited to gain administrative access to the database containing quarantined messages for review and certain configuration information (only version 6.0 and later).

  NOTE: In version 6.0, administrative access was restricted to localhost. However,

this restriction is not present on systems prior to this version and is also not imposed on prior versions upgraded to version 6.0 without a clean install.

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

References:

Original Advisory:
http://securityresponse.symantec.com/avcenter/security/Content/2005.05.31a.html

Product HomePage:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=642

Other references:
http://secunia.com/advisories/15562/

CVE Reference: None

❖ 15207 Symantec Brightmail AntiSpam UPX Parsing Engine Buffer Overflow Vulnerability (Remote File Checking)

ISS X-Force has reported a vulnerability in Symantec Brightmail AntiSpam, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the DEC2EXE parsing engine used by the antivirus scanning functionality when processing UPX compressed files. This can be exploited to cause a heap-based buffer overflow via a specially crafted UPX file.

Successful exploitation allows execution of arbitrary code.

The vulnerability affects the following products:
* Symantec BrightMail AntiSpam 4.0
* Symantec BrightMail AntiSpam 5.5

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

References:

Original Advisory:
http://www.sarc.com/avcenter/security/Content/2005.02.08.html
http://xforce.iss.net/xforce/alerts/id/187

Product HomePage:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=642

Other references:
http://secunia.com/advisories/14179/
http://www.kb.cert.org/vuls/id/107822

CVE Reference: CAN-2005-0249

❖ 15208 Symantec AntiVirus Scan Engine 4.x UPX Parsing Engine Buffer Overflow Vulnerability (Remote File Checking)

ISS X-Force has reported a vulnerability in Symantec AntiVirus Scan Engine 4.x, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the DEC2EXE parsing engine used by the antivirus scanning functionality when processing UPX compressed files. This can be exploited to cause a heap-based buffer overflow via a specially crafted UPX file.

Successful exploitation allows execution of arbitrary code.

The vulnerability affects the following products:
Symantec AntiVirus Scan Engine 4.0.X all versions
Symantec AntiVirus Scan Engine 4.3.X prior to build 4.3.3

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

References:

Original Advisory:
http://www.sarc.com/avcenter/security/Content/2005.02.08.html
http://xforce.iss.net/xforce/alerts/id/187

Product HomePage:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=173

Other references:
http://secunia.com/advisories/14179/
http://www.kb.cert.org/vuls/id/107822

CVE Reference: CAN-2005-0249

❖ 15209 Symantec AntiVirus Scan Engine 4.x RAR Archive Virus Detection Bypass Vulnerability (Remote File Checking)

André Jerleke has reported a vulnerability in Symantec AntiVirus Scan Engine 4.x, which can be exploited by malware to bypass certain scanning functionality.

The vulnerability is caused due to an error in the Symantec Antivirus component when processing encoded or archived content. This can be exploited to crash the decomposer component when parsing a specially crafted RAR file.

Successful exploitation causes malware inside the RAR file to bypass the scanning functionality.

This vulnerability primarily poses a risk in environments where virus scanning only is performed on gateway systems, as the malware still is detected by the RealTime Virus Scan / Auto-Protect functionality when extracted on systems running Symantec Antivirus.

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

References:

Original Advisory:
http://securityresponse.symantec.com/avcenter/security/Content/2005.04.27.html

Product HomePage:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=173

Other references:
http://secunia.com/advisories/15153/

CVE Reference: CAN-2005-1346

❖ 15211 Symantec Mail Security for Exchange 4.x RAR Archive Virus Detection Bypass Vulnerability (Remote File Checking)

André Jerleke has reported a vulnerability in Symantec Mail Security for Exchange 4.x, which can be exploited by malware to bypass certain scanning functionality.

The vulnerability is caused due to an error in the Symantec Antivirus component when processing encoded or archived content. This can be exploited to crash the decomposer component when parsing a specially crafted RAR file.

Successful exploitation causes malware inside the RAR file to bypass the scanning functionality.

This vulnerability primarily poses a risk in environments where virus scanning only is performed on gateway systems, as the malware still is detected by the RealTime Virus Scan / Auto-Protect functionality when extracted on systems running Symantec Antivirus.

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

References:

Original Advisory:
http://securityresponse.symantec.com/avcenter/security/Content/2005.04.27.html

Product HomePage:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=66

Other references:
http://secunia.com/advisories/15153/

CVE Reference: CAN-2005-1346

❖ 15212 Symantec Mail Security for Exchange 4.x UPX Parsing Engine Buffer Overflow Vulnerability (Remote File Checking)

ISS X-Force has reported a vulnerability in Symantec Mail Security for Exchange 4.x, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to a boundary error in the DEC2EXE parsing engine used by the antivirus scanning functionality when processing UPX compressed files. This can be exploited to cause a heap-based buffer overflow via a specially crafted UPX file.

Successful exploitation allows execution of arbitrary code.

The vulnerability affects the following products:
* Symantec Mail Security for Microsoft Exchange 4.0 (prior to build 4.0.10.465)
* Symantec Mail Security for Microsoft Exchange 4.5 (prior to build 4.5.3)

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

References:

Original Advisory:
http://www.sarc.com/avcenter/security/Content/2005.02.08.html
http://xforce.iss.net/xforce/alerts/id/187

Product HomePage:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=66

Other references:
http://secunia.com/advisories/14179/
http://www.kb.cert.org/vuls/id/107822

CVE Reference: CAN-2005-0249

❖ 15213 FutureSoft TFTP Server 2000 Directory Traversal Vulnerability (Remote File Checking)

Tan Chew Keong has reported a vulnerability in TFTP Server 2000, which can be exploited by malicious people to gain knowledge of sensitive information or compromise a vulnerable system.

Missing input validation can be exploited to access arbitrary files outside the TFTP root via directory traversal attacks.

The vulnerability have been reported in version 1.0.0.1. Other versions may also be affected.

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

References:

Original Advisory:
http://www.security.org.sg/vuln/tftp2000-1001.html

Product HomePage:
http://www.futuresoft.com/products/lit-tftp2000.htm

Other references:
http://secunia.com/advisories/15539/

CVE Reference: None

❖ 15214 FutureSoft TFTP Server 2000 Buffer Overflows Vulnerability (Remote File Checking)

Tan Chew Keong has reported a vulnerability in TFTP Server 2000, which can be exploited by malicious people to gain knowledge of sensitive information or compromise a vulnerable system.

Boundary errors within the handling of Read and Write requests can be exploited to cause a stack-based buffer overflow via a request containing an overly long filename or transfer-mode string.

Successful exploitation allows execution of arbitrary code with SYSTEM privileges.

The vulnerability have been reported in version 1.0.0.1. Other versions may also be affected.

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

References:

Original Advisory:
http://www.security.org.sg/vuln/tftp2000-1001.html

Product HomePage:
http://www.futuresoft.com/products/lit-tftp2000.htm

Other references:
http://secunia.com/advisories/15539/

CVE Reference: None

❖ 15627 SPA-PRO Mail @Solomon IMAP Directory Traversal Vulnerability

Tan Chew Keong has reported a vulnerability in SPA-PRO Mail @Solomon, which can be exploited by malicious users to gain knowledge of sensitive information or compromise a vulnerable system.

Missing input validation in the IMAP service can be exploited via various commands to view other users' mails, delete empty directories, rename directories, or create arbitrary directories via directory traversal attacks.

Successful exploitation allows execution of arbitrary code. **TC Impact:** Gather Info

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

References:

Initial Advisory :
http://www.security.org.sg/vuln/spa-promail4.html

Other references:
http://secunia.com/advisories/15573/

Product HomePage:
http://www.e-postinc.jp/solomon.htm

CVE Reference: None

❖ **15628 SPA-PRO Mail @Solomon IMAP Buffer Overflow Vulnerability**

Tan Chew Keong has reported a vulnerability in SPA-PRO Mail @Solomon, which can be exploited by malicious users to gain knowledge of sensitive information or compromise a vulnerable system.

A boundary error in the IMAP service when handling the CREATE command can be exploited to cause a buffer overflow by passing an overly long argument (about 260 bytes).

Successful exploitation allows execution of arbitrary code.

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

References:

Initial Advisory :
http://www.security.org.sg/vuln/spa-promail4.html

Other references:
http://secunia.com/advisories/15573/

Product HomePage:
http://www.e-postinc.jp/solomon.html

CVE Reference: None

New Vulnerabilities found this Week

❖ **Nortel VPN Routers IKE Packet Handling Denial of Service**
"Denial of Service"

NTA-Monitor has reported a vulnerability in Nortel VPN Routers, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to an error in the handling of IKE packets and can be exploited via a specially crafted IKE packet containing a malformed

ISAKMP header.

Successful exploitation causes the VPN router to crash or reboot.

The vulnerability has been reported in the 600, 1010, 1050, 1100, 1600, 1700, 1740, 2600, 2700, 4500, 4600, and 5000 models.

References:
http://www.nta-monitor.com/news/vpn-flaws/nortel/vpn-router-dos/

❖ **SPA-PRO Mail @Solomon IMAP Directory Traversal and Buffer Overflow**
"Execution of arbitrary code"

Tan Chew Keong has reported two vulnerabilities in SPA-PRO Mail @Solomon, which can be exploited by malicious users to gain knowledge of sensitive information or compromise a vulnerable system.

1) Missing input validation in the IMAP service can be exploited via various commands to view other users' mails, delete empty directories, rename directories, or create arbitrary directories via directory traversal attacks.

2) A boundary error in the IMAP service when handling the CREATE command can be exploited to cause a buffer overflow by passing an overly long argument (about 260 bytes).

Successful exploitation allows execution of arbitrary code.

References:
http://www.security.org.sg/vuln/spa-promail4.html

❖ **Symantec Brightmail AntiSpam Static Database Password**
"Bypass security restrictions"

A security issue has been reported in Symantec Brightmail AntiSpam, which can be exploited by malicious people to bypass security restrictions.

The security issue is caused due to a static database administration password, which can be exploited to gain administrative access to the database containing quarantined messages for review and certain configuration information (only version 6.0 and later).

NOTE: In version 6.0, administrative access was restricted to localhost. However, this restriction is not present on systems prior to this version and is also not imposed on prior versions upgraded to version 6.0 without a clean install.

References:
http://securityresponse.symantec.com/avcenter/security/Content/2005.05.31a.html

❖ **FutureSoft TFTP Server 2000 Directory Traversal and Buffer Overflows**
"Stack-based buffer overflow; Arbitrary code with SYSTEM privileges"

Tan Chew Keong has reported some vulnerabilities in TFTP Server 2000, which can be exploited by malicious people to gain knowledge of sensitive information or compromise a vulnerable system.

1) Boundary errors within the handling of Read and Write requests can be exploited to cause a stack-based buffer overflow via a request containing an overly long filename or transfer-mode string.

Successful exploitation allows execution of arbitrary code with SYSTEM privileges.

2) Missing input validation can be exploited to access arbitrary files outside the TFTP root via directory traversal attacks.

The vulnerabilities have been reported in version 1.0.0.1. Other versions may also be affected.

References:
http://www.security.org.sg/vuln/tftp2000-1001.html

❖ **qmail Memory Corruption Vulnerability**
"Corrupt memory"

Georgi Guninski has reported a vulnerability in qmail, which can be exploited by malicious people to compromise a vulnerable system.

A signedness error in the "commands()" function in commands.c can be exploited to corrupt memory via specially crafted data passed via qpopup/qpop3d or potentially qmail-smtpd.

Successful exploitation allows execution of arbitrary code, but only affects 64-bit systems with about 10GB of virtual memory.

Various types of other errors, which also potentially can be exploited to execute code, have also been reported.

The vulnerability has been reported in version 1.0.3. Other versions may also be affected.

References:
http://www.guninski.com/where_do_you_want_billg_to_go_today_4.html

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