netVigilance

ScoutNews Team **May 27 2005**
Issue # 21

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Eeye is hurt by sluggish market, watch out for bit-nappers, the spooks are getting into the hacking business, hero hackers? And Firefox gets anti-phishing.

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

- **Eeye cuts 29% of workforce**

Eeye Digital Security announced that they were laying-off 29 percent of their staff due to unrealized revenue expectations.

Red Herring

Full Story :
http://www.redherring.com/Article.aspx?a=12140&hed=Security+Startup+Makes+Cuts&sector=Industries&subsector=SecurityAndDefense

- **Latest threat: Bit-Napping: Hackers holding your data for ransom**

In a story relating to last weeks ScoutNews report on hacker shakdowns; we now have a new term; Bit-Napping.

Hackers gain access to an organizations network, encrypt vital data living on their systems and attempt to extort money to provide the de-encryption key.

Detroit News

Related Links :

http://www.detnews.com/2005/techcolumns/0505/25/tech-192155.htm

http://www.techworld.com/security/news/index.cfm?NewsID=3726

http://www.signonsandiego.com/news/computing/20050525-9999-1b25webs.html

- **Covert US hacker unit capable of launching cyber-war on US enemies.**

The US government has formed a Joint Functional Component Command for Network Warfare, or JFCCNW. It is reported to be made up of personnel from the CIA, National Security Agency, FBI, the four military branches, a smattering of civilians and military intelligence experts from allied countries.

It is also rumored that the CIA has been involved in exercises in simulating and responding to a cyber-attack against US assets.

Wired

Related Links:

http://www.wired.com/news/privacy/0,1848,67223,00.html?tw=wn_story_related

http://www.webpronews.com/news/ebusinessnews/wpn-45-20050526CIAWarGamesSimulateElectronicAssault.html

- **Whitehats resort to vigilante justice; hacking the hackers**

Security experts; apparently fed up with the proliferation of Phishing sites, has taken matters into their own hands and actually launched attacks against fraudulent banking sites.

At least two organizations have taken credit for defacing fake bank sites used in Phishing scams, call themselves ‘hero hackers’.

Yahoo

Related Links:

http://news.yahoo.com/s/afp/20050525/od_afp/usinternetsecurity_050525175347

- **Anti-Phishing toolbar available for Firefox**

The U.K.-based Web security company Netcraft has released it's anti-phishing toolbar for the popular Firefox browser. Netcraft claims to have blocked 7,000 phishing sites with this technology.
TechWeb News

Related Links:

http://www.informationweek.com/story/showArticle.jhtml;jsessionid=UJEGV2ZDKFIRYQSNDBCCKHSCJUMEKJVN?articleID=163701053&tid=6004

New Vulnerabilities Tested in SecureScout

- **15203 Netscape "IFRAME" JavaScript URLs Arbitrary HTML Execution Vulnerability (Remote File Checking)**

  A vulnerability has been reported in Netscape, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a user's system.

  The problem is that "IFRAME" JavaScript URLs are not properly protected from being executed in context of another URL in the history list. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site.

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

  References:

  Original Advisory:
  http://www.mozilla.org/security/announce/mfsa2005-42.html

  Product HomePage:
  http://channels.netscape.com/ns/browsers/default.jsp

  Other references:
  http://secunia.com/advisories/15437/
  http://secunia.com/advisories/15292/
  http://www.kb.cert.org/vuls/id/534710
  http://www.kb.cert.org/vuls/id/64875

  CVE Reference: CAN-2005-1476, CAN-2005-1477

- **15204 Netscape "IconURL" parameter in "InstallTrigger.install()" Verification Vulnerability (Remote File Checking)**

  A vulnerability has been reported in Netscape, which can be exploited by

malicious people to conduct cross-site scripting attacks and compromise a user's system.

Input passed to the "IconURL" parameter in "InstallTrigger.install()" is not properly verified before being used. This can be exploited to execute arbitrary JavaScript code with escalated privileges via a specially crafted JavaScript URL.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/mfsa2005-42.html

Product HomePage:
http://channels.netscape.com/ns/browsers/default.jsp

Other references:
http://secunia.com/advisories/15437/
http://secunia.com/advisories/15292/
http://www.kb.cert.org/vuls/id/534710
http://www.kb.cert.org/vuls/id/648758

CVE Reference: CAN-2005-1476, CAN-2005-1477

❖ **15205** **avast! Antivirus Device Driver Memory Overwrite Vulnerability (Remote File Checking)**

Piotr Bania has reported a vulnerability in avast! Antivirus, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or gain escalated privileges.

The vulnerability is caused due to missing input validation in the device driver and can be exploited to overwrite arbitrary memory via signals with specially crafted input.

Successful exploitation allows execution of arbitrary code with escalated privileges.

The vulnerability has been reported in version 4.6. Other versions may also be affected.

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

References:

Original Advisory:

http://pb.specialised.info/all/adv/avast-adv.txt

Product HomePage:

http://www.avast.com/eng/avast_4_professional.html

Other references:

http://secunia.com/advisories/15495/

CVE Reference: None

❖ **15596** **Qpopper user supplied config and trace files Privilege Escalation Vulnerability**

A vulnerability has been reported in Qpopper, which can be exploited by malicious, local users to perform certain actions with escalated privileges.

An error where user supplied config and trace files are processed with escalated privileges, can be exploited to create or overwrite arbitrary files.

The vulnerability has been reported in version 4.0.5. Prior versions may also be affected.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Low** Risk: **Gain Root**

References:

Original Advisory:
http://www.gentoo.org/security/en/glsa/glsa-200505-17.xml

Other references:
http://secunia.com/advisories/15475/

Product HomePage:
http://www.eudora.com/products/unsupported/qpopper/index.html

CVE Reference: CAN-2005-1151, CAN-2005-1152

❖ **15597** **Qpopper group or world-writable Files Creation Vulnerability**

A vulnerability has been reported in Qpopper, which can be exploited by malicious, local users to perform certain actions with escalated privileges.

The error can be exploited to create group or world-writable files.

The vulnerability has been reported in version 4.0.5. Prior versions may also be affected.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Low** Risk: **Gain Root**

References:

Original Advisory:
http://www.gentoo.org/security/en/glsa/glsa-200505-17.xml

Other references:

http://secunia.com/advisories/15475/

Product HomePage:
http://www.eudora.com/products/unsupported/qpopper/index.html

CVE Reference: CAN-2005-1151, CAN-2005-1152

❖ **15598** **IMail IMAP Service LSUB commands and NULL characters Vulnerability**

A vulnerability has been reported in IMail Server, which can be exploited to gain knowledge of sensitive information, cause a DoS (Denial of Service), or compromise a vulnerable system.

An error in the IMAP4d32 service when parsing LSUB commands can be exploited to consume all available CPU resources by passing a long string of NULL characters.

The vulnerability has been reported in version 8.13. Other versions may also be affected.

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

References:

Initial Advisory :
http://www.ipswitch.com/support/imail/releases/imail_professional/im82hf2.html

Other references:
http://www.idefense.com/application/poi/display?id=241&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=242&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=243&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=244&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=245&type=vulnerabilities
http://secunia.com/advisories/15483/

Product HomePage:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference: CAN-2005-1249, CAN-2005-1252, CAN-2005-1254, CAN-2005-1255, CAN-2005-1256

❖ **15599** **IMail IMAP Service SELECT commands and overly long mailbox name Vulnerability**

A vulnerability has been reported in IMail Server, which can be exploited to gain knowledge of sensitive information, cause a DoS (Denial of Service), or compromise a vulnerable system.

A boundary error in the IMAP4d32 service can be exploited to crash the service via a SELECT command with an overly long mailbox name (about 260 bytes).

The vulnerability has been reported in version 8.13. Other versions may also be affected.

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

References:

Initial Advisory :
http://www.ipswitch.com/support/imail/releases/imail_professional/im82hf2.html

Other references:
http://www.idefense.com/application/poi/display?id=241&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=242&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=243&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=244&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=245&type=vulnerabilities
http://secunia.com/advisories/15483/

Product HomePage:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference: CAN-2005-1249, CAN-2005-1252, CAN-2005-1254, CAN-2005-1255, CAN-2005-1256

❖ **15624** **IMail IMAP Service LOGIN commands and overly long mailbox name Vulnerability**

A vulnerability has been reported in IMail Server, which can be exploited to gain knowledge of sensitive information, cause a DoS (Denial of Service), or compromise a vulnerable system.

Boundary errors in the IMAP4D32 service when parsing LOGIN commands can be exploited to cause buffer overflows by passing either an overly long username (about 2,000 bytes) or an overly long username starting with certain special characters.

Successful exploitation allows execution of arbitrary code with SYSTEM privileges.

The vulnerability has been reported in version 8.13. Other versions may also be affected.

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

References:

Initial Advisory :
http://www.ipswitch.com/support/imail/releases/imail_professional/im82hf2.html

Other references:
http://www.idefense.com/application/poi/display?id=241&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=242&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=243&type=vulnerabilities

http://www.idefense.com/application/poi/display?id=244&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=245&type=vulnerabilities
http://secunia.com/advisories/15483/

Product HomePage:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference: CAN-2005-1249, CAN-2005-1252, CAN-2005-1254, CAN-2005-1255, CAN-2005-1256

❖ **15625** **IMail IMAP Service STATUS commands and overly long mailbox name Vulnerability**

A vulnerability has been reported in IMail Server, which can be exploited to gain knowledge of sensitive information, cause a DoS (Denial of Service), or compromise a vulnerable system.

A boundary error in the IMAP4D32 service when parsing STATUS commands can be exploited to cause a stack-based buffer overflow by passing an overly long string as mailbox name to the command.

Successful exploitation allows execution of arbitrary code with SYSTEM privileges.

The vulnerability has been reported in version 8.13. Other versions may also be affected.

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

References:

Initial Advisory :
http://www.ipswitch.com/support/imail/releases/imail_professional/im82hf2.html

Other references:
http://www.idefense.com/application/poi/display?id=241&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=242&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=243&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=244&type=vulnerabilities
http://www.idefense.com/application/poi/display?id=245&type=vulnerabilities
http://secunia.com/advisories/15483/

Product HomePage:
http://www.ipswitch.com/Products/IMail_Server/index.html

CVE Reference: CAN-2005-1249, CAN-2005-1252, CAN-2005-1254, CAN-2005-1255, CAN-2005-1256

❖ **18115** **MailEnable Unspecified SMTP Authentication 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 an unspecified error in the SMTP authentication and can be exploited to crash the SMTP service.

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

References:

Original advisory:
http://secunia.com/advisories/15487/

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

CVE Reference: None

New Vulnerabilities found this Week

- **CA Multiple Products Vet Antivirus Engine Buffer Overflow**
  "Execution of arbitrary code"

  Alex Wheeler has reported a vulnerability in various Computer Associates products, which can be exploited by malicious people to compromise a vulnerable system.

  The vulnerability is caused due to an integer overflow in the Vet Antivirus Engine (VetE.dll) when analyzing OLE streams. This can be exploited to cause a heap-based buffer overflow via e.g. a specially crafted Microsoft Office document.

  Successful exploitation allows execution of arbitrary code.

  The vulnerability affects the following products:
  * CA InoculateIT 6.0 (all platforms, including Notes/Exchange)
  * eTrust Antivirus r6.0 (all platforms, including Notes/Exchange)
  * eTrust Antivirus r7.0 (all platforms, including Notes/Exchange)
  * eTrust Antivirus r7.1 (all platforms, including Notes/Exchange)
  * eTrust Antivirus for the Gateway r7.0 (all modules and platforms)
  * eTrust Antivirus for the Gateway r7.1 (all modules and platforms)
  * eTrust Secure Content Manager (all releases)
  * eTrust Intrusion Detection (all releases)
  * BrightStor ARCserve Backup (BAB) r11.1 Windows
  * eTrust EZ Antivirus r6.2 - r7.0.5
  * eTrust EZ Armor r1.0 - r2.4.4
  * eTrust EZ Armor LE r2.0 - r3.0.0.14
  * Vet Antivirus r10.66 and below

  References:

http://www.rem0te.com/public/images/vet.pdf
http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=32896

- **WEB-DAV Linux File System No Enforcing of UNIX Permissions**
"Bypass certain security restrictions"

Andrew Pimlott has reported a security issue in WEB-DAV Linux File System (davfs2), which can be exploited by malicious, local users to bypass certain security restrictions.

The problem is that a mounted file system fails to support UNIX permissions. This can be exploited to manipulate and disclose then contents of arbitrary files on the file system.

References:
http://secunia.com/advisories/15497/

- **avast! Antivirus Device Driver Memory Overwrite Vulnerability**
"Denial of Service"

Piotr Bania has reported a vulnerability in avast! Antivirus, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or gain escalated privileges.

The vulnerability is caused due to missing input validation in the device driver and can be exploited to overwrite arbitrary memory via signals with specially crafted input.

Successful exploitation allows execution of arbitrary code with escalated privileges.

The vulnerability has been reported in version 4.6. Other versions may also be affected.

References:
http://pb.specialised.info/all/adv/avast-adv.txt

- **Qpopper Privilege Escalation Vulnerabilities**
"Escalated privileges"

Two vulnerabilities have been reported in Qpopper, which can be exploited by malicious, local users to perform certain actions with.

1) An error where user supplied config and trace files are processed with escalated privileges, can be exploited to create or overwrite arbitrary files.

The vulnerability has been reported in version 4.0.5. Prior versions may also be affected.

2) An unspecified error can be exploited to create group or world-writable files.

References:
http://www.gentoo.org/security/en/glsa/glsa-200505-17.xml

- **Cisco Various Products Compressed DNS Messages Denial of Service**
"Denial of Service"

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

The vulnerability is caused due to an error in the DNS implementation during the decompression of compressed DNS messages and can be exploited via a specially crafted DNS packet containing invalid information in the compressed section.

Successful exploitation crashes a vulnerable device or causes it to function abnormally.

The vulnerability affects the following products:
* Cisco IP Phones 7902/7905/7912
* Cisco ATA (Analog Telephone Adaptor) 186/188
* Cisco Unity Express

The following Cisco ACNS (Application and Content Networking System) devices are also affected:
* Cisco 500 Series Content Engines
* Cisco 7300 Series Content Engines
* Cisco Content Routers 4400 series
* Cisco Content Distribution Manager 4600 series
* Cisco Content Engine Module for Cisco 2600, 2800, 3600, 3700, and 3800 series Integrated Service Routers.

References:
http://www.cisco.com/warp/public/707/cisco-sn-20050524-dns.shtml
http://www.niscc.gov.uk/niscc/docs/al-20050524-00433.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