netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 26

June 30, 2006

Table of Contents

Product Focus

Messenger Service Vulnerability Scanner – The Messenger Service Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft Windows Messenger Service flaw (MS03-043).

This Week in Review

18 million spam emails less per day – well, so far so good. Computer Security taking 1st place in companies' concerns, still network protection not sufficient.

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

- **Korean Zombie King Busted. Suspect alleged to have sent 18 million spams per day**

SophosLabs have announced that the South Korean authorities have arrested a man suspected of running a 16,000-strong network of zombie computers. According to the

state-backed Korea Information Security Agency (KISA), the man is believed to have sent 18 million spam emails to 133 countries every day from his network (or botnet) of compromised computers.

Working with the police, KISA identified a man who has been running the botnet of 16,000 computers for the last six months using it to send out large amounts of loan-related spam.

SecurityNewsPortal

Full Story :
http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanEE%2edb&command=viewone&id=92&op=t

❖ Data Security Displacing Malware as #1 Concern Worldwide

Data Security was the top concern of enterprise IT professionals according to the results of a recently released survey sponsored by Apani Networks, a provider of software that secures inside the network perimeter.

The results were compiled by a third party, Infosurv Market Research, for the first of an ongoing series of surveys aimed at investigating IT security issues and concerns within enterprises worldwide. This week, the company released the results of its first confidential online survey of enterprise security professionals.

Results were based on 591 respondents worldwide and covered questions in the areas of data protection, security policies, network segmentation, de-perimeterization, IT security implementation and attack profiles.

IT Observer

Full Story :

http://www.it-observer.com/news.php?id=6547

❖ Being an IT security manager is like refereeing a World Cup match

What are the similarities between ITSec managers and a World Cup referee? There are more than you might imagine. While it's unlikely that anyone will shout rude chants that question your parentage or eyesight, you can be sure that similar sentiments may sometimes be muttered under users' breath. And while no-one will thank you when you've done a great job, everyone will be on your case if things take an unexpected turn for the worse.

Just like referees, IT managers have to keep a cool head and keep control of an ever-changing and volatile situation. Both have to quickly make sense of events as they occur, and make the right decisions quickly in accordance with rules and policies. Neither can afford to be partisan to one team: both have to be dispassionate observers of events, faithful only to the rules of the game.

Both have only limited resources available to them – the referee his 3 linesman, the IT director or manager and his team – yet both need to deliver a firm response to address the situation at all times, whether it's an isolated incident or a full-scale melee.

Securitypark.net

Full Story :
http://www.securitypark.co.uk/article.asp?articleid=25548&CategoryID=1

- **Is Your Network Protected? Not Remotely**

Organisations are opening up corporate network to hackers by not securing remote workers...

Organisations are not protecting their networks, according to research carried out by SafeNet, the leader in security and encryption. Passwords are still the most common security measure for mobile working, with 71 per cent relying on it, and yet it has long been known that this alone is an inadequate and risky security measure.

Over 50 per cent of organisations support mobile working for more than one in ten employees and 20 per cent of organisations support remote working for over 50 per cent of staff. The research, carried out over 1,200 IT managers and security professionals, also showed that 60 per cent used VPNs, 23 per cent digital certificates and only 10 per cent used smart cards.

"Traditional company borders are now a thing of the past, as more employers and employees see the benefit of remote working," said Gary Clark, VP EMEA, SafeNet. "But with thousands of people connecting from outside the corporate firewall, more appropriate security measures are needed to protect sensitive business information."

IT Backbones

Full Story :
http://www.theitshield.com/pr/8517

New Vulnerabilities Tested in SecureScout

- **12016 Cisco Access Point Web-browser Interface Vulnerability (CSCsd67403)**

The Cisco web-browser interface for Cisco access points contains a vulnerability that could, under certain circumstances, remove the default security configuration from the managed access point and allow administrative access without validation of administrative user credentials.

Successful exploitation of this vulnerability will result in unauthorized administrative access to the access point via the web management interface or via the console port.

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

References:

http://www.cisco.com/en/US/products/products_security_advisory09186a00806cd92f.shtml

CVE Reference:

❖ 12017 Cisco Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack (CSCsb77324)

The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

A malicious user may be able to send a small series of crafted HTTP packets to a concentrator which will cause the device to halt and drop user connections. The power must then be reset on the device to recover.

The vulnerability affects devices running software version 4.7.2.x < 4.7.2.B.

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

References:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_security_advisory09186a00805f0147.shtml

CVE Reference:

❖ 12030 Cisco VPN 3000 Concentrator, TCP connections resources consumptions (CSCsd26340)

The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication.

The concentrator does not manage TCP connections to port 80 aggressively enough, leading to a scenario where memory and other resources are consumed with open connections. In specific scenarios, the concentrator will stall and drop user connections. The device must then be restarted via console access or by resetting power on the device. Alternatively, the device will recover automatically within about 20 minutes, however during this time the device is unavailable except via console access.

The vulnerability affects devices running software version:
4.7.X < 4.7.2.F.
4.1.X < 4.1.7.L.

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

References:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_security_advisory09186a00805f0147.shtml

CVE Reference:

❖ 12112 Cisco IOS Stack Group Bidding Protocol Crafted Packet DoS

(CSCsb11124)

The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

Successful exploitation of this vulnerability may cause the affected device to become unresponsive and trigger a hardware reset, resulting in a denial of service condition.

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

References:

http://www.cisco.com/en/US/products/products_security_advisory09186a00805e8a63.shtml

CVE Reference:

❖ 12115 Cisco Access Point Memory Exhaustion from ARP Attacks (CSCsc16644)

A vulnerability exists in Cisco Aironet Wireless Access Points (AP) running IOS which may allow a malicious user to send a crafted attack via IP address Resolution Protocol (ARP) to the Access point which will cause the device to stop passing traffic and/or drop user connections.

Successful exploitation of this vulnerability may result in a denial of service (DoS) impacting the availability of the Wireless Access Point. Management and packet forwarding services will be unavailable.

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

References:

http://www.cisco.com/en/US/products/products_security_advisory09186a00805e465b.shtml

CVE Reference:

❖ 14732 Mozilla Firefox "contentWindow.focus()" Deleted Object Reference Vulnerability (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a user's system.

The vulnerability is caused due to a reference to a deleted object when designMode is enabled. This can be exploited to corrupt the memory and cause a crash by calling the "contentWindow.focus()" method on a container with specially crafted content.

Successful exploitation may allow execution of arbitrary code.

The vulnerability has been reported in versions 1.5 through 1.5.0.2.

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

References:

Original advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-30.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-1993

❖ 14733 Mozilla Firefox Exception Handling Full Path Disclosure Weakness (Remote File Checking)

A weakness has been discovered in Firefox, which can be exploited by malicious people to disclose system information.

The weakness is caused due to file path information being included in certain exceptions being thrown by the browser. This can e.g. be exploited to disclose the full installation path by calling the "window.sidebar.addSearchEngine()" JavaScript function with invalid parameters.

This may reportedly also be exploited to disclose the full path to the user's profile via errors thrown in installed extensions.

The weakness has been confirmed in version 1.5.0.3. Other versions may also be affected.

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

References:

Original advisory:
https://bugzilla.mozilla.org/show_bug.cgi?id=267645

Other references:
BUGTRAQ:20060521 Firefox 1.5.0.3 Flaw - Page can obtain path to Mozilla installation or profile by examining JavaScript exceptions
URL: http://www.securityfocus.com/archive/1/archive/1/434696/100/0/threaded
MISC: https://bugzilla.mozilla.org/attachment.cgi?id=164547
SECUNIA:20244
URL: http://secunia.com/advisories/20244
SECUNIA:20255
URL: http://secunia.com/advisories/20255
SECUNIA:20256
URL: http://secunia.com/advisories/20256
XF:mozilla-javascript-path-disclosure(26667)
URL: http://xforce.iss.net/xforce/xfdb/26667

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-2613

❖ 14734 Mozilla Firefox error in the sandbox protection of JavaScript (Remote File Checking)

A vulnerability has been reported in Firefox, which can be exploited by malicious people to bypass certain security restrictions.

An error in the sandbox protection of JavaScript run via EvalInSandbox can be exploited to execute arbitrary JavaScript code with escalated privileges by calling the "valueOf()" function on external objects outside of the sandbox.

Successful exploitation requires that the attacker is able to execute JavaScript code inside the EvalInSandbox (e.g. via a Proxy Autoconfig script or a third-party extension using the vulnerable functionality).

The weakness has been confirmed in version 1.5.0.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-31.html

Other references:
BUGTRAQ:20060602 rPSA-2006-0091-1 firefox thunderbird
URL:http://www.securityfocus.com/archive/1/archive/1/435795/100/0/threaded
GENTOO:GLSA-200606-12
URL:http://www.gentoo.org/security/en/glsa/glsa-200606-12.xml
GENTOO:GLSA-200606-21
URL:http://www.gentoo.org/security/en/glsa/glsa-200606-21.xml
SUSE:SUSE-SA:2006:035
URL:http://www.novell.com/linux/security/advisories/2006_35_mozilla.html
UBUNTU:USN-296-1
URL:http://www.ubuntulinux.org/support/documentation/usn/usn-296-1
UBUNTU:USN-297-1
URL:http://www.ubuntulinux.org/support/documentation/usn/usn-297-1
BID:18228
URL:http://www.securityfocus.com/bid/18228
FRSIRT:ADV-2006-2106
URL:http://www.frsirt.com/english/advisories/2006/2106
SECTRACK:1016202
URL:http://securitytracker.com/id?1016202
SECTRACK:1016214
URL:http://securitytracker.com/id?1016214
SECUNIA:20376
URL:http://secunia.com/advisories/20376
SECUNIA:20382

URL:http://secunia.com/advisories/20382
SECUNIA:20561
URL:http://secunia.com/advisories/20561
SECUNIA:20709
URL:http://secunia.com/advisories/20709

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-2787

❖ 14735 Mozilla Firefox errors in the browser engine, a memory corruption Vulnerability (Remote File Checking)

Some errors in the browser engine can be exploited to cause a memory corruption.

Successful exploitation may allow execution of arbitrary code.

The weakness has been confirmed in version 1.5.0.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-32.html

Other references:
* BUGTRAQ:20060602 rPSA-2006-0091-1 firefox thunderbird
* URL:http://www.securityfocus.com/archive/1/archive/1/435795/100/0/threaded
* CONFIRM: http://www.mozilla.org/security/announce/2006/mfsa2006-32.html
* GENTOO:GLSA-200606-12
* URL:http://www.gentoo.org/security/en/glsa/glsa-200606-12.xml
* GENTOO:GLSA-200606-21
* URL:http://www.gentoo.org/security/en/glsa/glsa-200606-21.xml
* SUSE:SUSE-SA:2006:035
* URL:http://www.novell.com/linux/security/advisories/2006_35_mozilla.html
* UBUNTU:USN-296-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-296-1
* UBUNTU:USN-297-1
* URL:http://www.ubuntulinux.org/support/documentation/usn/usn-297-1
* CERT-VN:VU#466673
* URL:http://www.kb.cert.org/vuls/id/466673
* CERT:TA06-153A
* URL:http://www.us-cert.gov/cas/techalerts/TA06-153A.html
* BID:18228
* URL:http://www.securityfocus.com/bid/18228
* FRSIRT:ADV-2006-2106
* URL:http://www.frsirt.com/english/advisories/2006/2106
* SECTRACK:1016202
* URL:http://securitytracker.com/id?1016202
* SECTRACK:1016214

* URL:http://securitytracker.com/id?1016214
* SECUNIA:20376
* URL:http://secunia.com/advisories/20376
* SECUNIA:20382
* URL:http://secunia.com/advisories/20382
* SECUNIA:20561
* URL:http://secunia.com/advisories/20561
* SECUNIA:20709
* URL:http://secunia.com/advisories/20709

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-2780

❖ 14736 Mozilla Firefox errors in the handling of specially crafted HTTP responses, arbitrary code execution (Remote File Checking)

Two errors in the handling of specially crafted HTTP responses in certain situations can be exploited to cause the browser to process a response as two separate responses from different sites.

Successful exploitation allows execution of arbitrary HTML and script in a user's browser session in context of an arbitrary site, but requires that the browser is configured to use a proxy or that the malicious site shares the same IP address as the targeted site.

The weakness has been confirmed in version 1.5.0.3. Other versions may also be affected.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-33.html

Other references:
BUGTRAQ:20060602 rPSA-2006-0091-1 firefox thunderbird
URL:http://www.securityfocus.com/archive/1/archive/1/435795/100/0/threaded
GENTOO:GLSA-200606-12
URL:http://www.gentoo.org/security/en/glsa/glsa-200606-12.xml
GENTOO:GLSA-200606-21
URL:http://www.gentoo.org/security/en/glsa/glsa-200606-21.xml
SUSE:SUSE-SA:2006:035
URL:http://www.novell.com/linux/security/advisories/2006_35_mozilla.html
UBUNTU:USN-296-1
URL:http://www.ubuntulinux.org/support/documentation/usn/usn-296-1
UBUNTU:USN-297-1
URL:http://www.ubuntulinux.org/support/documentation/usn/usn-297-1
BID:18228
URL:http://www.securityfocus.com/bid/18228
FRSIRT:ADV-2006-2106

URL:http://www.frsirt.com/english/advisories/2006/2106
SECTRACK:1016202
URL:http://securitytracker.com/id?1016202
SECTRACK:1016214
URL:http://securitytracker.com/id?1016214
SECUNIA:20376
URL:http://secunia.com/advisories/20376
SECUNIA:20382
URL:http://secunia.com/advisories/20382
SECUNIA:20561
URL:http://secunia.com/advisories/20561
SECUNIA:20709
URL:http://secunia.com/advisories/20709

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-2786

New Vulnerabilities found this Week

Mac OS X Update Fixes Multiple Vulnerabilities

"Stack-based buffer overflow; Arbitrary code execution; Crash the service"

Apple has issued an update for Mac OS X, which fixes multiple vulnerabilities.

1) An error in the AFP server within the handling of users' search results can be exploited by malicious users to gain knowledge of the names of files and folders for which the user performing the search has no access to.

2) A vulnerability within the Freshclam command line utility in ClamAV can potentially be exploited to compromise a vulnerable system.

3) A boundary error in ImageIO within the handling of TIFF images can be exploited to cause a stack-based buffer overflow. This crashes an affected application and may allow arbitrary code execution when a specially crafted TIFF image is viewed.

4) A format string error within the logging functionality of the setuid program "launchd" can be exploited by local users to execute arbitrary code with system privileges.

5) An error within "slapd" of the OpenLDAP server when handling an anonymous bind operation can be exploited to crash the service via a malformed ldap-bind message.

References:
http://docs.info.apple.com/article.html?artnum=303973

Cisco Wireless Access Point Web Management Vulnerability

"Bypass certain security restrictions"

A vulnerability has been reported in Cisco Wireless Access Point, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an error within the web management interface when

the Admin Access configuration has been changed from "Default Authentication" to "Local User List Only". This causes the access point to be re-configured with no security enabled, thus allowing open access to the access point via the web interface or via the console port with no validation of user credentials.

Successful exploitation requires that the web management interface is enabled.

The vulnerability has been reported in the following products when running Cisco IOS Software Release 12.3(8)JA or 12.3(8)JA1:
* 350 Wireless Access Point and Wireless Bridge
* 1100 Wireless Access Point
* 1130 Wireless Access Point
* 1200 Wireless Access Point
* 1240 Wireless Access Point
* 1310 Wireless Bridge
* 1410 Wireless Access Point

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060628-ap.shtml
http://descriptions.securescout.com/tc/12016

F-Secure Antivirus Products Scanning Bypass Vulnerability
“Bypass the scanning functionality”

Two vulnerabilities have been reported in various F-Secure Antivirus products, which can be exploited by malware to bypass the scanning functionality.

1) An unspecified error within the handling of executable programs where the name has been manipulated in a certain way can be exploited to bypass the anti-virus scanning functionality.

2) An error causes files on removable media to not be scanned when the "Scan network devices" option has been disabled.

Successful exploitation of the vulnerabilities bypasses the real-time scanning functionality and may result in execution of malware on the system.

References:
http://www.f-secure.com/security/fsc-2006-4.shtml

PHP "error_log()" Safe Mode Bypass Weakness
“Bypass the safe mode protection”

Maksymilian Arciemowicz has discovered a weakness in PHP, which can be exploited by malicious, local users to bypass certain security restrictions.

The weakness is caused due to an input validation error in the "error_log()" PHP function in the processing of the destination parameter. This can be exploited to bypass the safe mode protection via directory traversal attacks in the "php://" wrapper.

The weakness has been confirmed in version 5.1.4 and has also been reported in version 4.4.2. Other versions may also be affected.

References:
http://securityreason.com/achievement_securityalert/41

Mutt IMAP Namespace Buffer Overflow Vulnerability
"Denial of Service"

TAKAHASHI Tamotsu has reported a vulnerability in Mutt, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a user's system.

The vulnerability is caused due to a boundary error within the "browse_get_namespace()" function in browse.c. This can be exploited to cause a stack-based buffer overflow when processing an overly long namespace from the IMAP server.

Successful exploitation crashes the application and may allow arbitrary code execution, but requires that the user connects to a malicious IMAP server.

The vulnerability has been reported in version 1.4.2.1. Prior versions may also be affected.

References:
http://dev.mutt.org/cgi-bin/gitweb.cgi?p=mutt/.git;a=commit;h=dc0272b749f0e2b102973b7ac43dbd3908507540

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