netVigilance

ScoutNews Team **June 24, 2005**
Issue # 25

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Phishing threatens online transactions, Citadel offers form of early warning, MS lagging on browser security, CFOs worry about data security, regulatory compliance is serious business and eeye upgrades CardSystems after attack.

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

- **Security fears stifle ecommerce, online banking**

The recent spate of data security breaches in the banking industry has had a cooling effect on internet commerce and online banking according to a Gartner report issued on Thursday.

Although it is too early to predict the economic impact, the trend threatens to ripple through banks and any other agency that sees to reduce costs by utilizing email account management.

TechWeb News

Full Story :
http://www.securitypipeline.com/news/164902340;jsessionid=WUJXNUGSSQOZSQSNDBCSKHSCJUM

EKJVN

❖ Free service for daily briefing of internet Securtiy Breaches

The 2 minute warning service from Citadel Security will inform you of the most critical threats to the safety of your network.

Related Links :

www.citadel.com/2minutewarning

❖ Microsoft has no plans to eliminate pop-up attacks

Microsoft does not intend to fix a IE Browser vulnerability that enables Java scripts to be used in particular Phishing attacks.
A Java script pop-up that appears in front of a legitimate site spoofs users into thinking the pop-up is associated with the actual site.

Both Opera and Mozilla have added enhancements to prevent this type of attack.
CNET News.com

Full Story:
http://news.zdnet.com/2100-1009_22-5759894.html?tag=zdfd.newsfeed

❖ Information Security top concern for CFOs

Information security became the chief technology concern among CFOs for the first time in the seventh annual Technology Issues for Financial Executives survey. The survey, conducted by Computer Sciences Corp. (CSC) in association with the Financial Executives Research Foundation (FERF), found that recent events in the news about data theft has raised concern about cyber-security.

CFOs join CIOs from a 2005 Robert Half survey in identifying information security as their primary concern.
Computing South Africa

Full Story:

http://security.itworld.com/4977/050621is/page_1.html

❖ The Cost of a HIPAA violation: Your Career

While both HIPAA and Sarbanes-Oxley carry jail time as a possible penalty; the likelihood of an IT professional doing time is fairly slim.

This does not mean that IT professionals are immune. Consider the scenario where your boss gets indicted on a HIPAA violation, do you really think that IT will not be held responsible when his or her replacement 'cleans house'?

IT professionals need to be all the more vigilant where regulatory compliance is concerned. Regardless of the actions of the executive ultimately held accountable, those responsible for data security must err on the side of caution and document that security policies were followed.
Source

Related Links:
http://www.networkworld.com/research/2005/053005-jail.html
http://www.computerworld.com/securitytopics/security/story/0,10801,102665,00.html
http://www.symtym.com/index.php/hipaa_felon/

❖ I would 'upgrade' too…

Eeye customer CardSystems Inc. hacked to the tune of 40 million credit card records, had their security software upgraded after the breach. I just hope it's not too late.

Related Link:
http://seattletimes.nwsource.com/APWires/tech/D8ATKLM81.html

New Vulnerabilities Tested in SecureScout

❖ 13246 AOL Instant Messenger AddExternalApp Remote Buffer Overflow Vulnerability (Remote File Checking)

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

AOL Instant Messenger (AIM) is a real time messaging service.

The vulnerability exists in the way that AIM parses an AddExternalApp request with a TLV (type, length, value) type of greater than 0x2711. This type of request is prone to a buffer overflow which could allow a remote user to obtain the same privileges of the user who is currently logged on.

It is important to note that there is currently no way for an AIM user to block this type of request.

**AOL has made modifications to their AIM servers to prevent this vulnerability from being exploited through their servers. However, the underlying problem still exists in the client software which could still be exploited using something similar to a man in the middle attack. This could also be exploited if the attacker can contrive a way to bypass the filters on the AIM servers.

Vulnerable: AOL Instant Messenger 4.8.2646

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/271182

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/4677/info

CVE Reference: CAN-2002-0362, CVE-2002-0362

❖ 13247 AOL Instant Messenger Data Interception Vulnerability (Remote File Checking)

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

It is reportedly possible for a remote attacker to force a direct connection or file transfer with an AOL Instant Messenger (AIM) client. This may be exploited to intercept data the client is sending.

Vulnerable: AOL Instant Messenger 4.8.2646

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/269006

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/4574/info

CVE Reference: CAN-2002-0592

❖ 13248 AOL Instant Messenger Hyperlink Denial Of Service Vulnerability (Remote File Checking)

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

AOL Instant Messenger (AIM) is a real time messaging service. The AIM client runs on Microsoft Windows operating systems.

It is possible to crash the AIM client by sending a specially formatted hyper-link to a user. When the user attempts to launch the malicious hyper-link, the client will crash.

This issue appears to be caused by an unchecked buffer in the AIM software. As a result, it may also be possible to exploit this issue to cause attacker-supplied instructions to be executed on the machine of a user running the vulnerable client.

Vulnerable: AOL Instant Messenger 4.8.2646

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

References:

Original advisory:
http://www.safehack.com/Advisory/aimbuffer.txt

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/4244/info

CVE Reference: None

❖ 15629 Opera Dialog Origin Spoofing Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious web sites to spoof dialog boxes.

The problem is that JavaScript dialog boxes do not display or include their origin, which allows a new window to open e.g. a prompt dialog box, which appears to be from a trusted site.

Successful exploitation normally requires that a user is tricked into opening a link from a malicious web site to a trusted web site.

The vulnerability has been confirmed in version 8.0. Prior versions may also be affected.

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

References:

Original advisory:
http://secunia.com/secunia_research/2005-8/

Other references:
http://secunia.com/advisories/15488/

Product HomePage:
http://www.opera.com/download/

CVE Reference: None

❖ 15630 Opera Redirection Cross-Site Scripting Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious people to conduct cross-site scripting attacks against users.

The vulnerability is caused due to input not being sanitised, when Opera generates a temporary page for displaying a redirection when "Automatic redirection" is disabled (not default setting).

NOTE: A variant of this issue was first discovered in Opera versions 6.x and 7.x, but was reintroduced with the release of Opera 8.

The vulnerability has been confirmed in version 8.0.

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

References:

Original advisory:
http://secunia.com/secunia_research/2003-1/

Other references:
http://secunia.com/advisories/15423/

Product HomePage:
http://www.opera.com/download/

CVE Reference: None

❖ 15631 Opera "javascript:" URL Cross-Site Scripting Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious people to conduct cross-site scripting attacks and to read local files.

The vulnerability is caused due to Opera not properly restricting the privileges of "javascript:" URLs when opened in e.g. new windows or frames.

The vulnerability has been confirmed in version 8.0. Other versions may also be affected.

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

References:

Original advisory:
http://secunia.com/secunia_research/2005-5/advisory/

Other references:
http://secunia.com/advisories/15411/

Product HomePage:
http://www.opera.com/download/

CVE Reference: CAN-2005-1669

❖ 15632 Opera XMLHttpRequest Security Bypass Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Opera, which can be exploited by malicious people to steal content or to perform actions on other web sites with the privileges of the user.

Normally, it should not be possible for the XMLHttpRequest object to access resources from outside the domain of which the object was opened. However, due to insufficient validation of server side redirects, it is possible to circumvent this restriction.

The vulnerability has been confirmed in version 8.0.

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

References:

Original advisory:
http://secunia.com/secunia_research/2005-4/advisory/

Other references:
http://secunia.com/advisories/15008/

Product HomePage:
http://www.opera.com/download/

CVE Reference: CAN-2005-1475

❖ 15633 Mozilla Dialog Origin Spoofing Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Mozilla, which can be exploited by malicious web sites to spoof dialog boxes.

The problem is that JavaScript dialog boxes do not display or include their origin, which allows a new window to open e.g. a prompt dialog box, which appears to be from a trusted site.

Successful exploitation normally requires that a user is tricked into opening a link from a malicious web site to a trusted web site.

The vulnerability has been confirmed in Mozilla 1.7.8. Prior versions may also be affected.

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

References:

Original advisory:
http://secunia.com/secunia_research/2005-11/

Other references:
http://secunia.com/advisories/15489/

Product HomePage:
http://www.mozilla.org/products/mozilla1.x/

CVE Reference: None

❖ 15634 Firefox Dialog Origin Spoofing Vulnerability (Remote File Checking)

Secunia Research has discovered a vulnerability in Firefox, which can be exploited by malicious web sites to spoof dialog boxes.

The problem is that JavaScript dialog boxes do not display or include their origin, which allows a new window to open e.g. a prompt dialog box, which appears to be from a trusted site.

Successful exploitation normally requires that a user is tricked into opening a link from a malicious web site to a trusted web site.

The vulnerability has been confirmed in FireFox 1.04. Prior versions may also be affected.

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

References:

Original advisory:
http://secunia.com/secunia_research/2005-11/

Other references:
http://secunia.com/advisories/15489/

Product HomePage:

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

CVE Reference: None

❖ 15635 AOL Instant Messenger Remote Buffer Overflow Vulnerability (Remote File Checking)

The remote host is using AOL Instant Messenger (AIM) - a p2p software, which may not be suitable for a business environment.

AOL Instant Messenger (AIM) is a real time messaging service.

The vulnerability exists in the way that AIM parses a game request with a TLV (type, length, value) type of 0x2711. This type of game request is prone to a buffer overflow which could allow a remote user to obtain the same privileges of the user who is currently logged on.

It is important to note that there is currently no way for an AIM user to block this type of request.

**AOL has made modifications to their AIM servers to prevent this vulnerability from being exploited through their servers. However, the underlying problem still exists in the client software which could still be exploited using something similar to a man in the middle attack or if an attacker can bypass the filters on the AIM servers.

Vulnerable: AOL Instant Messenger 4.8.2616

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

References:

Original advisory:
http://www.securityfocus.com/archive/1/247885

Product HomePage:
http://www.aim.com/get_aim/win/latest_win.adp

Other references:
http://www.securityfocus.com/bid/3769/info

CVE Reference: CVE-2002-0005

New Vulnerabilities found this Week

❖ SGI Advanced Linux Environment Multiple Updates

"Directory traversal attacks, extract files to arbitrary directories"

SGI has issued a patch for SGI Advanced Linux Environment. This fixes multiple vulnerabilities, which can be exploited by malicious people to disclose sensitive information, conduct directory traversal attacks, extract files to arbitrary directories, or potentially compromise a user's system.

References:
ftp://patches.sgi.com/support/free/security/advisories/20050603-01-U.asc

- **VERITAS NetBackup Request Packet Handling Denial of Service**
  "Denial of Service"

A vulnerability has been reported in VERITAS NetBackup for NetWare Media Servers, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a boundary error when handling request packets and can be exploited to cause a buffer overflow via a specially crafted request packet.

Successful exploitation crashes the application. Code execution is reportedly not possible.

References:
http://seer.support.veritas.com/docs/277485.htm

- **Linux Kernel Two Vulnerabilities**
  "Denial of Service"

Two vulnerabilities have been reported in the Linux kernel. One has an unknown impact, and the other can be exploited by malicious, local users to cause a DoS (Denial of Service).

1) An error exists in the handling of access to ar.rsc via ptrace and restore_sigcontext.

2) An error in the delivery of signals can cause a kernel panic when a sub-thread "exec" with a pending timer.

References:
http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.1

- **SGI IRIX arrayd Authentication Spoofing Vulnerability**
  "Execute arbitrary commands"

SGI has acknowledged a vulnerability in IRIX, which can be exploited by malicious people to compromise a vulnerable system.

The vulnerability is caused due to an error in arrayd during the processing of authentication requests when configured to use NONE or SIMPLE authentication. This can be exploited to execute arbitrary commands with root privileges on a vulnerable system.

Successful exploitation requires arrayd to be configured to use NONE or SIMPLE authentication.

References:
ftp://patches.sgi.com/support/free/security/advisories/20050604-01-A.asc

- **Whois.Cart Cross-Site Scripting and Local File Inclusion**
  "Cross-site scripting attacks"

Elzar Stuffenbach has reported two vulnerabilities in Whois.Cart, which can be exploited by malicious people to conduct cross-site scripting attacks and disclose sensitive information.

1) Input passed to the "page" parameter in "profile.php" isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

2) Input passed to the "language" parameter in "index.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from local resources.

The vulnerabilities have been reported in version 2.2 and prior. Other versions may also be affected.

- **Sun Solaris Perl Modules Two Vulnerabilities**
  "Cross-site scripting attacks"

Sun has acknowledged two vulnerabilities in Solaris, which can be exploited by malicious people to bypass certain security restrictions and conduct cross-site scripting attacks.

1) An error in the "Safe.pm" Perl module can be exploited to bypass certain compartment access controls.

2) Input passed to the "start_form()" function in the "CGI.pm" Perl module isn't properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

The vulnerabilities has been reported in Perl module "Safe.pm" version 2.0.7 and prior, and Perl module "CGI.pm" version 2.752 and prior.

References:
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101426-1

- ### Cisco VPN Concentrator Group Name Enumeration Weakness
  "Gain knowledge of certain information"

NTA Monitor has reported a weakness in Cisco VPN 3000 Concentrator, which can be exploited by malicious people to gain knowledge of certain information.

The problem is that the device returns different responses depending on whether or not a valid group name is supplied when the device is configured for group name authentication.

Once a valid group name is guessed, this can further be used to obtain the hash of the group password.

References:
http://www.nta-monitor.com/news/vpn-flaws/cisco/VPN-Concentrator/index.htm
http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/4_7/471con3k.htm

- ### Microsoft Internet Explorer Dialog Origin Spoofing Vulnerability
  "Spoof dialog boxes"

Secunia Research has discovered a vulnerability in Internet Explorer, which can be exploited by malicious web sites to spoof dialog boxes.

The problem is that JavaScript dialog boxes do not display or include their origin, which allows a new window to open e.g. a prompt dialog box, which appears to be from a trusted site.

Successful exploitation normally requires that a user is tricked into opening a link from a malicious web site to a trusted web site.

The vulnerability has been confirmed in a fully updated version 6.0. Prior versions may also be affected.

References:
http://secunia.com/secunia_research/2005-9/
http://www.microsoft.com/technet/security/advisory/902333.mspx

- ### OpenBSD "ip_ctloutput()" Denial of Service
  "Denial of Service"

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

The vulnerability is caused due to an error in the "ip_ctloutput()" function and can be exploited by using the "getsockopt()" function to retrieve IPsec credentials for a socket.

Successful exploitation causes a kernel panic.

References:
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.7/common/002_getsockopt.patch
ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.6/common/017_getsockopt.patch

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