netVigilance

ScoutNews Team **12 March 2004**

Issue #11

Weekly ScoutNews by netVigilance

Table of Contents

This Week in Review

Microsoft releases their monthly series of Windows patches. It seems that the security holes in Outlook were more dangerous than they first though. No doubt you have downloaded the patches and updated your entire network already. Check out the Jon Oltsik commentary on rethinking computer security. Then read about the latest catchphrase for next-generation data warehousing and how the Linux folks could learn something about network security from the mistakes and gains that Microsoft has made.

Top Security News Stories this Week

❖ **The Rethinking of Computer Security**

The security industry is in the midst of a transition, one that promises to profoundly change the way businesses think about the subject. In many respects, it parallels how the creation of the Web browser reshaped people's thinking about the potential of the Internet. Recall that the advent of the Web browser helped transform the Internet from a clubby insider research vehicle to an essential piece of the global business infrastructure. But the system also needed to become more reliable, easier to use, and better integrated into business processes before its potential could be reached. Similar demands now attend the field of information security thanks to the accelerating intersection of security and business. One sign of the changing times was on full display last month when Microsoft Chairman Bill Gates was invited to deliver the keynote speech at the RSA Security conference. Microsoft's record obviously stirs passions in the security industry, but there is little doubt that the company definitely gets it now. Check out the full text of this story. Insightful and informative.

http://www.pcworld.com/news/article/0,aid,115123,00.asp
By Jon Oltsik – ZDNet

❖ **Microsoft Issues Security Updates Patches Flaws in Outlook, Windows, and Messenger**

Microsoft continued its policy of releasing monthly security updates with three new software patches this week, including fixes for the MSN Messenger instant messaging program,

Windows Media Services, and the Outlook e-mail client. Microsoft published three security bulletins: MS04-008, MS04-009, and MS04-010. Only one of the security holes, in Outlook, could allow attackers to run malicious code on affected computers, and none of the new vulnerabilities was rated "critical" by Microsoft, the company says.

http://www.pcworld.com/news/article/0,aid,115123,00.asp
By Paul Roberts – IDG News

❖ **Outlook Flaw Riskier Than Thought**

Microsoft has raised the severity rating of an Outlook flaw to "critical," the highest level, after its initial analysis was challenged by the researcher who found the security hole. The vulnerability in Outlook 2002, first publicized on Tuesday, when Microsoft released a patch, could allow an attacker to use a malicious Web site to cause an affected PC to download and execute a program.

http://news.com.com/2100-1002_3-5172179.html?part=rss&tag=feed&subj=news
http://www.infoworld.com/article/04/03/10/HNrethinks_1.html
By Robert Lemos – C|NET / Paul Roberts – IDG News

❖ **Patching Pirates**

It seems that nobody wants to provide updates and patches to users of pirated software. Microsoft, the biggest malware and hacker target, won't allow the use of Windows Update to easily patch pirated copies of Windows. And AV and firewall vendors are famous for hiding patches for undisclosed vulnerabilities in their feature set upgrades and signature updates -- available only to paying customers.

Their disdain makes sense. According to the Business Software Alliance, more than 39 percent of all software is stolen. An IDC study found that every 1 percent of pirated software removes roughly $40 billion and 150,000 jobs from the global economy. Providing those users with security patches is akin to GM honoring extended service warranties for stolen cars.

http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss346_art673,00.html
By Larry Walsh – InfoSecurity

❖ **Microsoft to Automate Windows Security**

If you attended the RSA conference, you know about this already. In fact, if you read the ScoutNews two weeks ago, we gave you the scoop. This week, the Washington Post finally got around to talking the masses about it. Information latency is what we call it. As you know, Microsoft plans to release a new version of its popular Windows XP software that automatically downloads and installs software patches onto personal computers, one of the company's most aggressive moves to promote Internet safety. Starting in mid-2004, Windows XP customers will be able to download a new "service pack" that includes the automatic installation function. The software also will include a stronger Internet firewall, new protections against computer viruses and software that blocks Internet pop-up advertising. This may help all the home and small business users but Network Administrators know it will take a lot more than this to fend off the bad guys. Also check out the UK Register's take on the upcoming Service Pack 2.

http://www.washingtonpost.com/wp-dyn/articles/A29328-2004Mar4.html
http://www.zone-h.com/en/news/read/id=4085/
http://www.theregister.co.uk/content/55/36123.html
By Brian Krebs - Washington Post / Zone-h / The Register

- **Security BI - The Latest Catchphrase For Next-generation Data Warehousing**

Quick: Your job as a security manager is to secure the:

A. Network
B. Applications
C. Data
D. Users

Actually, it's a trick question. The answer is none of the above. Your job is to secure the business. No problem, you say. I've got firewalls, DMZs, IDSes, authentication servers. Wrong answer. Securing the business isn't about point technologies or security architecture. It's not even about policy. It's about presenting security-relevant data in a business context. It's about cost-justifying decisions based on risk models, not unpredictable threats and arbitrary vulnerabilities. It's about framing the security message in a way that motivates the stakeholders who drive business strategy and sign security PO's. In short, it's about security business intelligence, the new buzz word of the month for security wonks.

http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss346_art677,00.html
By Andrew Briney - InfoSecurity

- **Model Security From Microsoft?**

It's not crazy to suggest that Linux could learn from Microsoft's example when it comes to security

In three months, Microsoft users will finally reap the benefits of the company's new focus on security. The release of the second major update to Windows XP answers many long-standing design criticisms of its operating system. But this was not a pain-free learning exercise. Indeed, Microsoft paid a steep price in the coin of user dissatisfaction -- and in some cases, lasting mistrust. Check out Robert Lemos' column on how Microsoft's focus on ease of security offers an instructive example for the Linux world.

http://comment.zdnet.co.uk/0,39020505,39148310,00.htm
By Robert Lemos – CNET News

New Vulnerabilities Tested in SecureScout

Six new vulnerability Test Cases have been incorporated into the SecureScout database this week. Of course, these weekly updates essential in keeping your network scanning tool one step in front of the hackers, inside or outside the organization.

- **11030 PPTP Server Version Disclosure Vulnerability**

The remote host is running a PPTP (VPN) service, this service allows remote users to connect to a private network. Server version (PPTP version), Hostname and Vendor string can be gathered by a malicious user.

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

CVE Link: No CVE link available
Counterpane: http://www.counterpane.com/pptp-faq.html
SecureScout Test Case: http://descriptions.securescout.com/tc/11030

- **14416 Vulnerability in Windows Media Services Could Allow A Denial of Service**

A vulnerability exists because of the way that Windows Media Station Service and Windows Media Monitor Service, components of Windows Media Services, handle TCP/IP connections. If a remote user were to send a specially-crafted sequence of TCP/IP packets to the listening port of either of these services, the service could stop responding to requests and no additional connections could be made. The service must be restarted to regain its functionality.

Windows Media Unicast Service may also be affected by a successful attack against Windows Media Station Service if Windows Media Unicast Service is sourcing a playlist from Windows Media Station Service. In this case, Windows Media Unicast Service could stop functioning when it encounters the next item in the playlist. An administrator can stream media by using Windows Media Unicast Service without a playlist.

Test Case Impact: **Gather Info** Vulnerability Impact: **Denial of Service** Risk: **Medium**

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0905
Microsoft: http://www.microsoft.com/technet/security/Bulletin/MS04-008.mspx
SecureScout Test Case: http://descriptions.securescout.com/tc/14416

- **14417 Vulnerability in MSN Messenger Could Allow Information Disclosure**

A security vulnerability exists in Microsoft MSN Messenger. The vulnerability exists because of the method used by MSN Messenger to handle a file request. An attacker could exploit this vulnerability by sending a specially crafted request to a user running MSN Messenger. If exploited successfully, the attacker could view the contents of a file on the hard drive without the user's knowledge as long as the attacker knew the location of the file and the user had read access to the file. To exploit this vulnerability, an attacker would have to know the sign-on name of the MSN Messenger user in order to send the request.

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

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0122
Microsoft: http://www.microsoft.com/technet/security/Bulletin/MS04-010.mspx
SecureScout Test Case: http://descriptions.securescout.com/tc/14417

- **17878 OWA Function Allows Unauthenticated User to Enumerate GlobalAddress**

List

Outlook Web Access (OWA) in Microsoft Exchange 5.5, SP4 and earlier, allows remote attackers to identify valid user email addresses by directly accessing a back-end function that processes the global address list (GAL).

Among the functions Outlook Web Access (OWA) in Exchange 5.5 offers is the ability to search the global address list (GAL). By design, this is an authenticated function, implemented as a two-tier architecture - a front tier that provides a user interface and a back-end tier that actually performs the search. However, only the front tier actually checks authentication. An attacker who sent a properly formatted request to the back-end function that actually performs the search could enumerate the GAL without authenticating.

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

CVE Link: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0660
Microsoft:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-047.asp
Security Focus: http://www.securityfocus.com/bid/3301
SecureScout Test Case: http://descriptions.securescout.com/tc/17878

- **19012 Adware Claria**

Adware: Software that brings ads to your computer. Such ads may or may not be targeted, but are "injected" and/or popup, and are not merely displayed within the form of an ad-sponsored application.

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

CVE Link: No CVE link available
PestPatrol: http://pestpatrol.com/pestinfo/C/Claria.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19012

- **19013 Exploit Alexa (Alexa-MSN Vulnerability)**

Your use of \%windir%\web\related.htm, which helps you located pages related to those found in a search, transmits the complete url of your search result to both "msn.com" and "alexa.com". In some cases this could contain sensitive information such as username, password, session id, search string, "secret paths", and more. The vulnerability has been confirmed for Internet Explorer 6 on Windows 2000 and Windows XP with all Service Packs and hotfixes.

The Alexa registry entry is created by an IE 6 install or installation of an IE Service Pack. It is nothing to worry about. It is simply a registry key that creates a menu item that points to a local web page that points to an MSN search page that uses the Alexa engine. The issue is the 'related links' feature of IE which appears as the 'Tools'/'Show Related Links' menu item, and a corresponding toolbar button if you added it (from the 'Customize...' link on the toolbar).

If you have removed this registry entry, it will be restored the next time you add a service pack for IE. Its absence does not cause any harm to IE's operation; its presence causes no real benefit. If you use 'related links', IE will contact the Alexa servers to obtain information about other web pages which might be related. But you will not be spied on UNLESS you intentionally install other Alexa software.

Test Case Impact: **Gather Info** Vulnerability Impact: **Full Log** Risk: **Medium**

CVE Link: No CVE link available
PestParol: http://pestpatrol.com/pestinfo/A/Alexa.asp
SecureScout Test Case: http://descriptions.securescout.com/tc/19013

New Vulnerabilities this Week

Microsoft Windows Media Services Remote Denial of Service Vulnerability
It has been reported that Microsoft Windows Media Services is prone to a remote denial of service vulnerability. This may allow an attacker to cause the services to effectively deny access to legitimate users by sending specially crafted TCP/IP packets on TCP ports 7007 and/or 7778.

Microsoft Windows Media Services 4.1 included with Microsoft Windows 2000 Server Service Pack 2, Service Pack 3, and Service Pack 4 is reported to be vulnerable to this issue. Windows Media Services 4.1 for Windows NT 4.0 is not vulnerable. SecureScout just happens to have a Test case for this.
For more information, see
http://securityresponse.symantec.com/avcenter/security/Content/9825.html
Source: Symantec

Microsoft Internet Explorer Cookie Path Restrictions Can Be Byassed By Remote Servers
A vulnerability was reported in Microsoft Internet Explorer (IE) in the processing of cookies. A remote user may be able to bypass the path restrictions specified by a cookie's originator. Several other browsers are also affected. It has been reported that a remote user (server) can employ a combination of path traversal and encoding techniques to bypass cookie path restrictions in the target user's browser. Malicious software on a server can obtain cookies from the target user's browser that should be restricted to a separate application path on the same server. The affected vendors were reportedly notified between July 12 and July 18, 2003.
Impact: A remote server application can obtain cookies from the target user's browser for the same domain but regardless of the path restrictions.
Solution: No solution has been publicly disclosed at the time of this entry.
For more information, see www.microsoft.com/technet/security/
http://www.securitytracker.com/alerts/2004/Mar/1009361.html
Source: Security Tracker

MyProxy Input Validation Hole Lets Remote Users Conduct Cross-Site Scripting Attacks
An input validation vulnerability was reported in MyProxy. A remote user can conduct cross-site scripting attacks. It seems that the proxy server does not filter HTML code from user-supplied HTTP requests. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will

originate from the site running the MyProxy software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.
Impact: A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the MyProxy software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.
Solution: The vendor plans to include a fix in the next released.
For more information, see http://www.securitytracker.com/alerts/2004/Mar/1009395.html
Source: Security Tracker

Multiple Vendor HTTP Response Splitting Vulnerability
A paper (Divide and Conquer - HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics) was released to describe various attacks that target web users through web application, browser, web/application server and proxy implementations. These attacks are described under the general category of HTTP Response Splitting and involve abusing various input validation flaws in these implementations to split HTTP responses into multiple parts in such a way that response data may be misrepresented to client users.

Exploitation would occur by injecting variations of CR/LF sequences into parts of HTTP response headers that the attacker may control or influence. The general consequences of exploitation are that an attacker may misrepresent web content to the client, potentially enticing the user to trust the content and take actions based on this false trust.

While the various implementations listed in the paper contribute to these attacks, this issue will most likely be exposed through web applications that do not properly account for CR/LF sequences when accepting user-supplied input that may be returned in server responses.

This vulnerability could also aid in exploitation of cross-site scripting vulnerabilities.
For more information, see http://www.securityfocus.com/bid/9804/discussion/
Source: Security Focus

Calife - Buffer Overflow Vulnerability
Calife, a popular Linux program which provides super user privileges to specific users, was found to contain a buffer overflow related to the getpass(3) library function. A local attacker could potentially exploit this vulnerability, given knowledge of a local user's password and the presence of at least one entry in /etc/calife.auth, to execute arbitrary code with root privileges.
For more information, see http://www.debian.org/security/2004/dsa-461
http://www.uniras.gov.uk/l1/l2/l3/brief2004/brief-11904.txt
Source: Debian

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 Americas and North 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